MeterWare for Windows
User's Guide

NAT

NETWORK

APPLICATION

TECHNOLOGY INC

NAT
NETWORK APPLICATION TECHNOLOGY INC

1686 Dell Avenue
Campbell, CA 95008-6901
Phone (408) 370-4300
Fax (408) 370-4222

support@nat.com
http://www.nat.com

Document No. 891–5260–13

September 1995

Copyright © 1995, Network Application Technology, Inc.

All rights reserved.

No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language in any form by any means without the written permission of N.A.T.

Licenses and Trademarks

EtherMeter is a registered trademark and, TokenMeter and MeterWare are trademarks of Network Application Technology, Inc. All other trademarks and trade names are the property of their respective holders.

Changes and Updates

Network Application Technology reserves the right to change or update the contents of this user's guide and to change the specifications of its products at any time without prior notification.

Every effort has been made to keep the information in this document current and accurate as of the date of publication or revision. However, no guarantee is given or implied that the document is error-free or that it is accurate with regard to any specification.

Network Application Technology, Inc.
1686 Dell Avenue
Campbell, CA 95008–6901

Phone: (408) 370-4300
Fax: (408) 370-4222
E-mail: support@nat.com

Printed in USA 2/6/96

Table of Contents

Chapter 1 *Introduction and Installation* 1

Textual Conventions 2
System Requirements 3
ODBC Overview 3
MeterWare Installation 4
MeterWare Application 5
ODBC 7

Chapter 2 *Start Up* 11

MeterWare Icons 11
Starting MeterWare 12
System and Device Configuration 13
Configuring MeterWare for NAC/102 Network Cards 13
Configuring WINSOCK Editions of MeterWare 14
Assigning Device Addresses 15
Configuring Devices with MeterWare's BOOTP Name Server 15
The Network Map 18
Tool Palettes 18
The Network Palette 18
The Draw Palette 19
Adding Devices to the Network Map . 19
Reviewing Device Status 20
Adding a Sub-LAN 20
Removing Devices 21
Connecting Devices on the Network Map . 21
Disconnecting Devices 21
Locking the Position of Devices 21
Identifying Devices 22
Locating Devices 22
Accessing RMON MIB Groups 23
Non-configured Devices Window 24

Chapter 3 *RMON Utilities* 25

Ethernet RMON Utilities 26
Token Ring RMON Utilities 27
Launching an Ethernet RMON Utility 29
RMON Statistics Window 30
Statistics - Errors View.....30
Statistics - Packet Distribution View ..32
Statistics - Packet Trend View 33
Statistics - Error Trend One View 33
Statistics - Error Trend Two View 34
RMON History Window 34
RMON Host Window Overview.....34
Host Window Views 35
RMON TopN Window Overview.....35
RMON Matrix Window Overview 36
RMON Alarm/Event Control Table Overview36
RMON Event Window Overview.....37
RMON Capture/Filter Overview 37
How to Access the Capture/Filter Window 37
The RMON Capture/Filter Window..38
Channel Tab (Capture/Filter Application)38
Filter Tab (Capture/Filter Application)41
Analyze Tab (Capture/Filter Application)42
Buffer Tab (Capture/Filter Application)44
Steps for Establishing a Basic Capture/Filter 46
Editing Channel Configuration 47
Viewing the RMON Filters, Channels and Buffers 48
Saving a Buffer and Viewing a Saved Trace File 48
Viewing a Saved Trace File.....48
Types of Filter Packets Allowed.....49
Editing Channel Configuration.....50
Creating a Channel.....51
Freeing Memory Resources 52
Viewing the RMON Filters, Channels and Buffers.....52
Launching a Token Ring RMON Utility 53
MAC-Layer Statistics Overview 54
.....MAC-Layer Stats - Events View54
MAC-Layer Stats - Error Window....55

MAC-Layer Stats - Packet View 57
Promiscuous Statistics Window 57
MAC-Layer History Window 58
Promiscuous History Window 58
Ring Station Window 58
Station Order Window 59
Station Configuration Window 59
Source Routing Window.....59

Chapter 4 *N.A.T. Extensions*..... 61

Accessing N.A.T.-specific applications 62
New Node Discovery Window.....62
NND Table.....62
Adding NND Control Entries.....63
NND Control Table Variables.....64
Modifying NND Control Entries 65
IP Mapping.....66
IP Mapping Table.....66
Adding IP Mapping Control Entries (EtherMeter Only) 66
Adding Addresses to the Router Table (EtherMeter Only) 67
Modifying IP Mapping Entries (EtherMeter Only) 68
IP Mapping Control Table Variables 69
Peak Statistics.....69
Top 10 Window (EtherMeter Only) 70
Selecting a Top 10 Category 70
Zoom View.....71
Protocols.....71
Token Ring Protocols 71
Ethernet Protocols Window Overview....71

Chapter 5 *SNMP Tools* 73

SNMP Templates.....74
GET and SET Commands.....75
SNMP DA Options 75
Pre-Defined SNMP Templates 76
RMON Templates 76
N.A.T. Enterprise Templates 77

SNMP Template Editor 78
Open an Existing Template 78
Create a New Template 80
Delete a MIB Variable 82
Add Tables to a Template 82
Save a Template 84
Template Editor Example 84
SNMP Utility 88
GET, SET and Search 90
SET Operations 91
Search the MIB Tree 93
SNMP Utility Examples 93
Example 1: GET and GET-NEXT 93
Example 2: Activate and Deactivate Tables 94
Reactivate Tables 97
Verify the Active Tables 97
MIB Compiler 98
MIB Compiler Run 100
MIB File Format 100
MIB Text Format 101
Warning Messages 102
Error Messages 103
Binary File Errors 105
Learn 106
Name Editor 108
Sort a Name Table 109
Edit a Name Table Online 109
Add a Name to the Table 110
Delete a Name from the Table 110
Edit a Name Table Off-line 110
ASCII File Layout 111
Value Column Format 112
Symbolic Name Format 112
Name Table Compiler 114

Chapter 6 *MeterWare Utilities* *115*

Locate a Device 116
System and Device Logs 117
Device Log Messages 118
Modify Log Parameters 118
Log Dump 120

Device Firmware Download 120
Firmware Files 121
Add Firmware Defaults 122
Download Firmware to a Device 122
Firmware Download Error Messages 124
Ping Device Window 126
MIB Poller 127
Enterprise View Window 129
Docking Bar 129
Dial Remote 129
Modem Trace 129

Chapter 7 *BootP Name Server* *131*

Router Considerations 132
BOOTP Device Configuration 132
Add Devices to the BOOTP Table 133
Save Configuration Data to Non-volatile Memory 135
Force Configuration Data Download 136
..... 137

Appendix A *Name Tables* *139*

Ethernet Types 139
Vendor Types 146

Appendix B *NAC/102 Installation* *159*

NAC/102 Jumper Settings 160
Ethernet Interface 161
Interrupt Request (IRQ) Settings 162

Appendix C *Your MTRWARE.INI File* *163*

Appendix D *Traps* *165*

Enterprise Specific Traps 166
Traps Defined for the RMON Group 166
Traps Defined for N.A.T. 167

Glossary *169*

Index *175*

Chapter 1 Introduction and Installation

Welcome and thank you for purchasing the new ***MeterWare for Windows*** network monitoring system from Network Application Technology (N.A.T.). MeterWare for Windows enables you to fully manage your N.A.T. EtherMeters and TokenMeters and stay one step ahead of your growing network. This chapter defines the environment required to use the MeterWare for Windows software package and describes the installation process.

The MeterWare Package

The MeterWare package includes:

- Three installation disks
- The *MeterWare for Windows User's Guide*

Textual Conventions

Listed below are the typographical conventions you will find throughout this guide:

TYPE STYLE	DESCRIPTION
Italics	The *italic* typeface indicates file names, directory names or operating system commands.
Exactly Opt	An ***Exactly Opt*** entry is optional, but must be typed exactly as indicated. The text is a 10-point, bold and italicized Courier font.
Exactly Req	An ***Exactly Req*** entry is required text and must be typed exactly as indicated. The text is a 10-point, bold, italicized and underlined Courier font.
`Variable Opt`	A `Variable Opt` entry is an optional text variable. When the text is actually entered, the desired data replaces the text variable. The text is a 10-point, Courier font.
`Variable Req`	A `Variable Req` entry is a required text variable. When the text is actually entered, the desired data replaces the text variable. The text is a 10-point, underlined Courier font.

System Requirements

The system requirements to run MeterWare are the following:

- 486 33MHz or better IBM PC or compatible
- DRAM: 8MB minimum
- Hard disk space: 8MB for installation
- Microsoft Windows™ 3.1 or Windows for Workgroups 3.11
- WINSOCK-compliant IP stack or N.A.T. NAC/102 card
- Color monitor (recommended)
- Disk cache (recommended)

  For example, DOS 6.2 includes a disk cache called SMARTDRV. Make sure the cache application (e.g., *smartdrive.exe*) is installed in your *autoexec.bat* file. The database operations in MeterWare are many times slower if no disk cache is installed in your system.

ODBC Overview

Microsoft's ODBC software provides a generic interface to various database file formats. By using Microsoft's ODBC software, you do not need to install the actual database application (e.g., Borland's dBASE IV) to be able to write to the database file format. ODBC writes to a generic file structure and then maps it to a data source filename.

Since MeterWare uses Microsoft's ODBC drivers, you must install and/or configure the appropriate ODBC database driver. N.A.T. provides you with the necessary Microsoft ODBC driver to write to the dBASE IV file format.

After you install the ODBC driver, you need to assign the appropriate N.A.T. data source filename to it. If you already have ODBC drivers installed, you will need to add the N.A.T. data source filename to your ODBC setup.

ODBC configuration for this application requires that a dBASE IV driver be configured for a data source named *MeterWare Device Data Source* and that a "Selected Directory" be specified to *\MTRWARE\DATABASE*.

NOTE: The data source must be the same string as listed above. (It is not case sensitive.)

To determine whether or not ODBC is installed on your machine, go into the Control Panel and look for an ODBC icon.

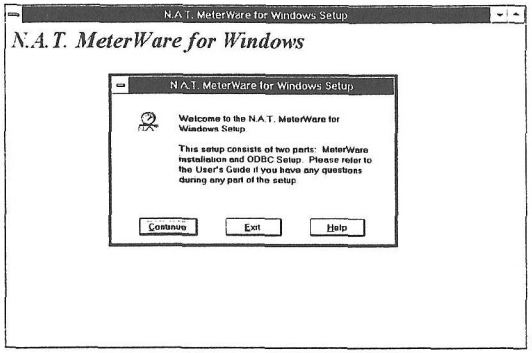
MeterWare Installation

To install MeterWare, follow the procedures below:

1. Place the "MeterWare Setup" disk #1 in the floppy disk drive.
2. Choose Run from the File menu in the Program Manager window.
3. Type *drive:setup* where *drive* is the letter denoting the disk drive containing disk #1.
4. Click OK.

   The N.A.T. MeterWare for Windows Setup window appears, as shown in Figure 1-1, "N.A.T. MeterWare for Windows Setup."

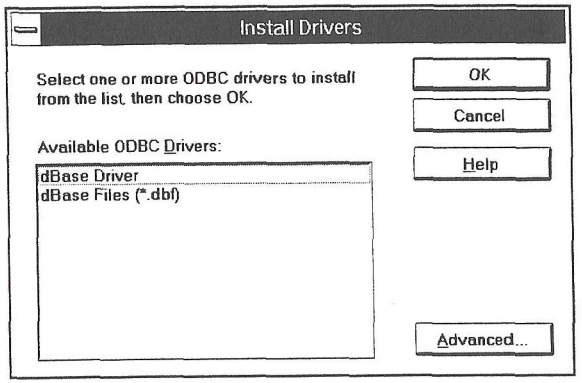
Figure 1-1 N.A.T. MeterWare for Windows Setup



5. Click Continue.

   The MeterWare for Windows Setup window appears, as shown in Figure 1-2, "MeterWare for Windows Setup."

Figure 1-2 MeterWare for Windows Setup

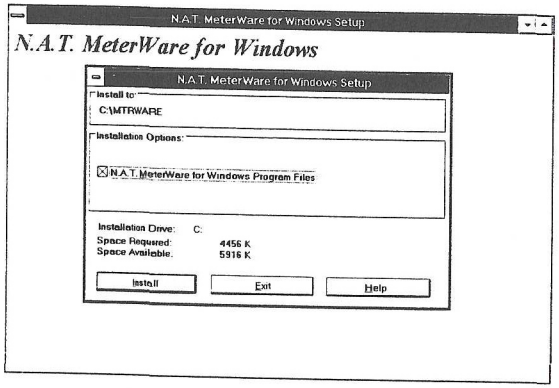


MeterWare Application

6. Type in the `directory` where you want to install MeterWare or accept the default *(C:\MTRWARE)*.
7. Click Continue.

   The MeterWare for Windows Setup window appears displaying the space requirements and where the program files are to be installed, as shown in Figure 1-3, "MeterWare for Windows Setup Window."

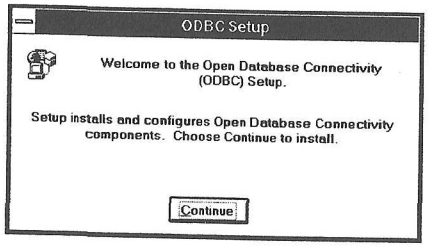
Figure 1-3 MeterWare for Windows Setup Window



8. Click Install.

   The installation program installs the program files for you. The ODBC Setup window appears, as shown in Figure 1-4, "ODBC Setup Window."

Figure 1-4 ODBC Setup Window

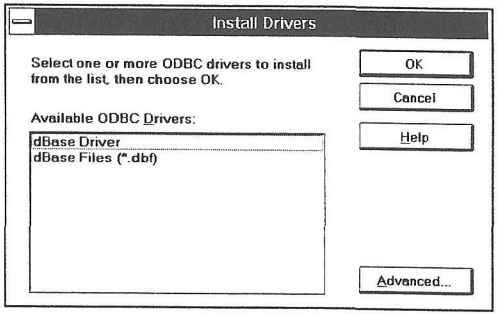


ODBC

1. Click Continue.

   A listing of the ODBC dBASE driver appears in the Install Drivers window, as shown in Figure 1-5, "Install Drivers."

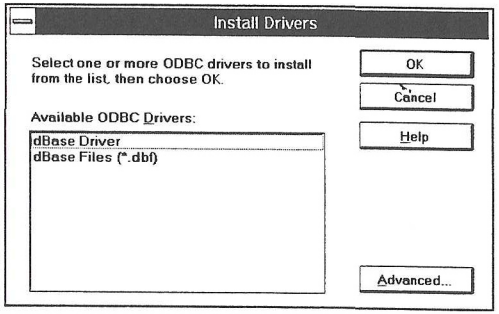
Figure 1-5 Install Drivers



2. Highlight the ODBC dBase Driver and click OK.

   The name of the corresponding N.A.T. data file (i.e., *MeterWare Device Data Source*) appears in the Data Sources window, as shown in Figure 1-6.

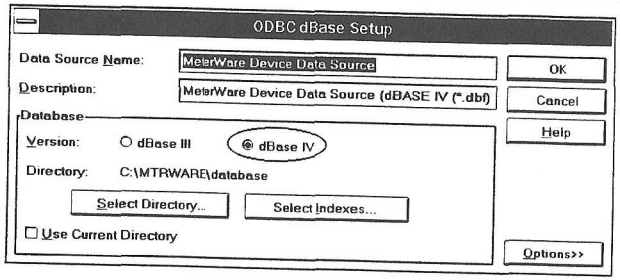
Figure 1-6 Data Sources



3. Verify that the dBASE driver you installed is dBASE IV. To verify the version installed, do the following:
   - Select the MeterWare Device Data Source driver listed on the Data Sources window.
   - Click Setup.

   The ODBC dBase Setup window appears, as shown in Figure 1-7, "ODBC dBase Setup."

Figure 1-7 ODBC dBase Setup



   - Verify the Version as dbase IV.

4. Click OK.

   You are returned to the Data Sources window.

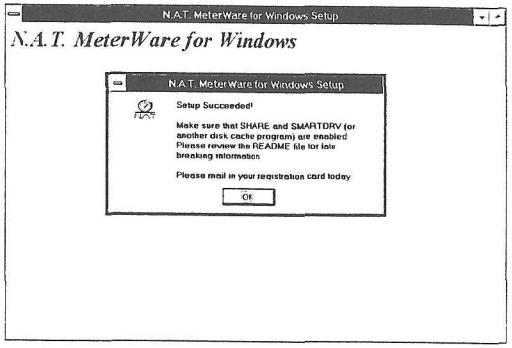
5. De-select "Use Current Directory."
6. Click on "Select Directory." Select */MTRWARE/database* and OK.
7. Click Close.

   The "Setup Succeeded" message appears.

8. Click OK.

   Upon complete installation, the "Setup Succeeded" message appears, as shown in Figure 1-8, "N.A.T. MeterWare for Windows Setup."

Figure 1-8 N.A.T. MeterWare for Windows Setup



9. Click OK.

   Now you're ready to start MeterWare.

10. Double-click the N.A.T. MeterWare for Windows icon.

    The first time you start MeterWare, you need to tell it which TCP/IP stack you're using.

11. Select the appropriate TCP/IP stack from the list box.

Chapter 2 Start Up

MeterWare provides a graphical interface to monitor and control multiple subnetworks from any location on the network. MeterWare displays subnetworks and nodes as icons on a graphical network map. The color of the status dot of a node icon indicates its real-time operational state. You monitor and control the network by choosing operations from the MeterWare menu and interacting directly, using your mouse, with subnetworks and node icons on the map.

This chapter provides basic start up instructions for using MeterWare.

MeterWare Icons

Once you install MeterWare, two icons appear under the MeterWare Program Group, as shown in Figure 2-1, "MeterWare Icons."

Figure 2-1 MeterWare Icons

The icons are described below:

- The N.A.T. MeterWare for Windows icon launches MeterWare.
- The Readme icon contains a text file with important operation information.

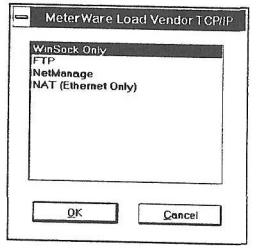
Starting MeterWare

To launch MeterWare, double–click on its icon in the MeterWare Program Group.

Upon first installation, you need to specify the IP stack you are using, as shown in Figure 2-2, "MeterWare Load Vendor TCP/IP Window."

1. Highlight the name of the appropriate vendor stack and choose OK. Your MTRWARE.INI stores the IP stack information. Refer to Appendix C for more information.

Figure 2-2 MeterWare Load Vendor TCP/IP Window



The NetMap window is displayed. By default, the NetMap window contains two other windows:

- The Network Map window

  Use the Network Map window to create a graphical representation of your network.

- The Non-Configured Devices window

  If the Network Manager finds devices on your network that are not configured in the Network Map window, it displays the devices in this window.

System and Device Configuration

Before MeterWare can manage devices, the MeterWare station and network devices must have network addresses (IP addresses). You must assign the MeterWare station and each device on the network a unique IP address. Depending on the network setup, you might also need to assign the MeterWare station and each device a subnet mask, a default router (gateway) IP address or both.

Configuring MeterWare for NAC/102 Network Cards

If you install MeterWare installed the NAC/102 network card, MeterWare opens the Network Configuration dialog box. Until you enter the IP address for the MeterWare station, MeterWare opens this dialog box every time you start the program.

To configure the main MeterWare station, do the following:

1. From the network map menu, choose Options\MW Configuration.
2. In the IP Address text box, type the `IP address` of the MeterWare station.
3. In the Network/Subnet Mask text box, type the `subnet mask` or accept the default.
4. If MeterWare is communicating through an IP router, type the `default router IP address` in the Gateway Router IP Address text box.
5. Choose OK to save these parameters.

During installation, MeterWare detects the Ethernet address of the NAC/102 card. You cannot change the hardware address in the Hardware Address text box.

Setup parameters include network addresses. MeterWare saves these setup parameters to the MeterWare station's hard disk. You do not have to repeat these setup procedures unless you change the MeterWare station's IP address.

If the MeterWare station will manage N.A.T. devices with serial communications capabilities (out-of-band), you need to configure these remote devices. (Refer to the Online Help Topic, "System Configuration," for step–by–step procedures.)

Configuring WINSOCK Editions of MeterWare

The WINSOCK edition of MeterWare automatically configures the MeterWare software, using parameters provided by the system it is communicating with.

The WINSOCK version of MeterWare uses other vendors' TCP/IP protocol stacks such as NetManage and ftp OnNet (other vendors' WINSOCK-compliant stacks are also supported by MeterWare). You must configure other vendors' network interface cards through their protocol stacks. Before running MeterWare, verify that the protocol stack (e.g., NetManage or ftp) is installed and functioning correctly. Refer to your ftp and NetManage documentation for information.

When you start MeterWare, it transfers configuration parameters from your TCP/IP protocol stack to the MeterWare station. To check this configuration, do the following:

1. From the network map menu, choose Options/MW Configuration.
   The Network Configuration window opens.
2. Check the following settings to make sure they match your TCP/IP protocol stack setup:
   - IP address
   - Hardware address
   - Subnet mask
   - Default router IP address

If the MeterWare station will manage N.A.T. devices with serial communications capabilities (out-of-band), you need to configure these remote devices. (Refer to the Online Help Topic, "System Configuration," for step–by–step procedures.)

As signing Device Addresses

To use MeterWare to manage devices using SNMP, each device on your network must be configured with a unique IP address. After assigning a unique IP address to a device, you must also assign your MeterWare station's IP address to the device before MeterWare can manage it. If additional MeterWare stations will also manage your network's devices, you must assign each additional station's IP address to each of the devices.

You can assign addresses to N.A.T. devices with any of the following:

- MeterWare
- An RARP or BOOTP server already residing on the network
- ASCII terminals (or PCs) attached to devices' serial ports

The following section describes how to configure devices using MeterWare Help only. Refer to the appropriate documentation for information on the other methods.

Configuring Devices with MeterWare's BOOTP Name Server

MeterWare uses its integrated BOOTP Name Server to assign the following addresses:

- Device IP addresses
- Managing host IP addresses
- Default router IP addresses to managed N.A.T. devices

You can use the BOOTP Name Server to configure devices in one of two ways:

- BOOTP Table
- SET Command

When you turn on devices connected to the network that have no configuration data (do not have IP addresses) in their non-volatile memory areas, they issue BOOTP requests. If configuration data for these devices is in the BOOTP Table, the BOOTP Name Server sends the data to them and icons for the devices appear on the network map.

If a device has configuration data in its non-volatile memory area, it does not issue a BOOTP request. To gain control of a preconfigured device through MeterWare, you can download configuration data from the BOOTP Table with the SET command (see below).

To add device configuration data to the BOOTP Name Server Table, do the following:

1. From the network map menu, choose Options/BOOTP Editor. The BOOTP Name Server dialog box opens.
2. Make sure the BOOTP Name Server is active. (An "X" appears in the Name Server Active box. If the BOOTP Name Server is not active, it does not respond to BOOTP requests. The Name Server Active box does not have to be checked to force an IP address download.
3. Choose Add.

   The BOOTP Address Entry dialog box opens.
4. In the Device Hardware text box, type the Ethernet or Token Ring MAC address of the device.
5. In the Device IP text box, type the IP address of the device.

   The text box defaults to the IP address of your MeterWare station.
6. In the Management Station (NMS) IP text box, type the IP address of the managing station.
7. Choose OK to return to the BOOTP Name Server dialog box.

When the BOOTP Name Server responds to a BOOTP request, it does not save the data to the device's non-volatile memory area. If the device is reset (turned off and on), the device reverts to its status before the BOOTP Name Server downloaded the data.

To save the data to the device's non-volatile memory area, do the following:

1. Double-click the device entry row in the BootP Table.
2. Select Save To Device (an "X" appears in the checkbox).
3. In the Router IP text box, type the IP address of the router.

   If the device is on the same LAN segment, this text box may be left blank. If the device is on another LAN segment, connected by a router capable of forwarding BOOTP request packets, enter the IP address of the router.
4. In the Agent Temporary IP text box, type a temporary IP address for the device.

   The temporary IP address is loaded into the volatile memory area of the device. The data in the Agent IP text box is loaded into non-volatile memory. Therefore, if you are configuring the device on a local LAN with the intent of moving the device to another LAN, use the temporary IP address to identify the device.
5. Choose OK to return to the BOOTP Name Server dialog box.
6. Choose Close to exit.

Configured devices do not broadcast BOOTP requests. To assign an IP address to and gain control of a device, download the device's configuration data from the BOOTP Table with a SET command.

N.A.T. devices have a password-protection feature that limits the ability of the BOOTP Name Server to issue a SET command. The device password prevents an unauthorized person from taking over a device. You must know the password to force a download of the configuration data.

To download configuration data, do the following:

1. Add the device to the BOOTP Name Server Table.
2. Select the table entry for the device.
3. Choose Set.
4. Type the device password and press Enter, or, if the device is not password-protected, press Enter.

   MeterWare sends the configuration data to the device, overwriting the device's non-volatile memory area.

Reviewing Device Status

MeterWare color codes the icons on the Network Map, so you can review the status of the network at a glance.

MeterWare shows the status of every device and subnet on the network defined in the database, using the following colors for the icon status dot:

- Green

  The device is responding to IP pings (ICMP echo packets) or SNMP Gets of the devices sysUptime MIB. For a subnet, all devices are okay.

- Red

  The device does not respond to a MeterWare poll. The intermediate network path to the device may be interrupted or a mechanical failure may have occurred in the device. For a subnet, at least one device is not responding.

- Yellow

  The device has sent a trap. For EtherMeters and TokenMeters, yellow indicates an alarm condition. For a subnet, at least one device has an alarm condition.

- Blue

  Indicates a non-IP device, or for a subnet, no SNMP or ping-able devices.

Adding a Sub-LAN

To add a sub-LAN to the network map, do the following:

1. Choose the Sub-LAN tool on the Network palette.
2. Click the Network Map window.
3. Enter a name for the sub-LAN, then choose OK.

   MeterWare displays a sub-LAN icon in the Network Map window.
4. Double-click the sub-LAN icon.

   MeterWare displays a window where you map the sub-LAN.

Removing Devices

Pointer Tool

To remove a device from the network map, do the following:

1. Choose the Pointer tool on the Network palette.
2. Click the device you want to remove.
3. Choose Edit/Delete to remove the device, or press the Delete key.

Connecting Devices on the Network Map

Connector Tool

You can connect devices to any of the following:

- Other devices
- Ethernet networks
- Token Ring networks

To connect devices on the network map, do the following:

1. Choose Window/Network Palette to display the Network palette, if it is not already visible.
2. Choose the Connector tool on the Network palette.
3. Click a device on the map, then drag the cursor to the network icon.

   MeterWare draws a connection between the device and the network or other device.

Disconnecting Devices

Disconnect Tool

To disconnect a device, do the following:

1. Choose Window/Network Palette to display the Network palette, if it is not already visible.
2. Choose the Disconnect tool on the Network palette.
3. Click the line that connects a device icon to the network icon.

Locking the Position of Devices

Lock Tool

1. Choose Window/Network Palette to display the Network palette, if it is not already visible.
2. Choose the Lock tool on the Network palette.
3. Click the device that you want to lock in position on the network map.

Identifying Devices

When you identify a device, you specify information about it in its Information tab. MeterWare stores this data in its database and uses it to identify and communicate with a device.

You do not need to identify network icons or sub-LANs.

To identify a device, do the following:

1. Double-click the device icon on the network map.
   MeterWare displays the device Information tab.
2. Enter the `IP Address` in the Information tab.
   If you have a host file configured for your IP stack, then you can resolve IP addresses by using the device names. See the IP stack vendor's documentation to create a host file.
3. Complete the rest of the Information tab:
   - If you are configuring an SNMP device that is connected to the network, choose Resolve IP.
     MeterWare gathers device information and completes the Information tab.
   - If you are configuring a non-SNMP device or a device that is not connected to the network, complete the Information tab manually.
4. Review the data in the Information tab and make any changes that are needed.

Locating Devices

You can search the main map and all submaps for a device by name, IP address or MAC address. The Network Map will scroll to the location of the device when it is found.

To search the network map for a device, do the following:

1. Choose Edit/Locate Device.
   MeterWare displays the Locate Device dialog box.
2. Choose a device from one of the list boxes.
3. Enter the search criteria, then choose OK.
   When MeterWare locates the device, it selects the device.

Accessing RMON MIB Groups

MeterWare supports the following Remote Network Monitoring Management Information Base (RMON MIB) object groups:

- Statistics evaluates the overall performance of a LAN segment
- Token Ring Statistics provides MAC-layer and LLC statistics for Token Ring segments
- Host shows the nodes on the LAN segment, the status of the nodes and the node traffic statistics
- Matrix maintains statistics for conversations between nodes
- History provides short-term historical views of network statistics
- Token Ring History provides a history of MAC-layer and LLC statistics for Token Ring segments
- Alarms sets thresholds on a particular statistic
- Events processes the alarm, based upon parameters in the Event table
- Capture collects network traffic between nodes that you specify
- Filter restricts the view of captured data to the items in which you are interested
- Token Ring Station provides statistics and status information associated with each station on the local ring
- Token Ring Station Order provides the order of the stations monitored on the ring
- Token Ring Configuration actively manages Token Ring stations
- Token Ring Source Routing provides utilization statistics derived from source routing information optionally present in Token Ring packets

MeterWare displays detailed statistics from each of the RMON MIB groups in a variety of windows. While the MeterWare station continues to monitor the network, you can save RMON statistics collected by MeterWare to a file and analyze these statistics in a word processor, spreadsheet or database program.

The following sections give an overview on how to use two of the RMON applications. For more detailed information, please refer to MeterWare's comprehensive online help system.

Non-configured Devices Window

If MeterWare receives a trap from a device that is not on its main map or on any subnet maps, a device is created and placed in the non-configured devices window. Later, you can cut and paste this device to the main map(s).

Chapter 3 RMON Utilities

MeterWare RMON utilities allow you to display detailed statistics for *RMON MIB* groups in a variety of graphical and tabular formats.

There are two sets of RMON utilities which you can use, depending upon your network:

- Ethernet RMON Utilities

  For a complete list of RMON utilities, refer to "Ethernet RMON Utilities," on page 26.

- Token Ring RMON Utilities

  For a complete list of Token Ring RMON utilities, refer to "Token Ring RMON Utilities," on page 27.

NOTE: Some of the RMON utilities are available for both Ethernet and Token Ring networks.

Ethernet RMON Utilities

The following table provides brief descriptions of the Ethernet RMON utilities. Refer to "Launching an Ethernet RMON Utility," on page 29 for more information.

UTILITY	DESCRIPTION	REFER TO...
Stats	Evaluates the overall performance of a LAN segment.	page 30
History	Provides long-term historical views of network statistics.	page 34
Host	Shows the nodes on the LAN segment and the status of those nodes. It also allows you to observe the traffic statistics for all nodes monitored on the network segment.	page 34
TopN	Helps you determine the stations generating the most traffic for a given parameter.	page 35
Matrix	Maintains statistics for conversations between devices (hosts).	page 36
Alarm	Sets threshold alarms for measurements based on utilization, packet rates, multicast error packets and other criteria.	page 36
Events	Lets you create and edit events.	page 37
Filter	Opens the Capture/Filter application.	page 37
Capture	Opens the Capture/Filter application.	page 37

Token Ring RMON Utilities

The following table provides brief descriptions of the Token Ring RMON utilities. Refer to "Launching a Token Ring RMON Utility," on page 53 for more information.

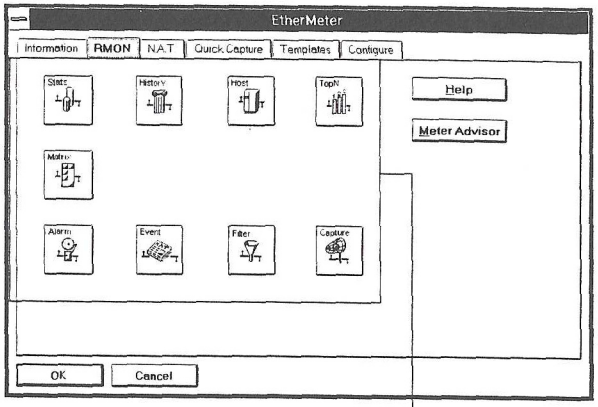
UTILITY	DESCRIPTION	REFER TO...
MAC Stats	Opens the MAC Statistics application, which displays statistics on normal, repeat-mode activity. These errors and statistics are specific to the Token Ring link layer protocol.	page 54
Prom Stats	Opens the Promiscuous Statistics application, which displays statistics on normal data packets.	page 57
MAC Hist	Opens the MAC History application, which displays a history of normal, repeat-mode activity.	page 58
Prom Hist	Opens the Promiscuous History application, which displays a history of data traffic on the ring.	page 58
Host	Opens the RMON Host application, which shows the nodes on the LAN segment and the status of those nodes. It also allows you to observe the traffic statistics for all nodes monitored on the network segment.	page 34
TopN	Opens the RMON TopN application, which helps you determine the stations generating the most traffic for a given parameter.	page 35
Matrix	Opens the RMON Matrix application, which maintains statistics for conversations between addresses (nodes).	page 36
Station	Opens the Station application, which displays detailed information about individual stations on the ring.	page 58
Order	Opens the Ring Order application, which displays a list of stations in the order of insertion to the ring. Use this application to determine where on the ring a specific station is located.	page 59
Config	Opens the Ring Configuration application, which displays detailed configuration information for stations monitored by this RMON agent.	page 59
Src. Route	Opens the Source Routing application, which displays data from the source routing information in the packets.	page 59

UTILITY	DESCRIPTION	REFER TO...
Alarm	Opens the Alarm/Event Control Table application, which sets threshold alarms for measurements based on utilization, packet rates, broadcast, multicast error packets and other criteria.	page 36
Event	Opens the Event Control Table application, which lets you create and edit events.	page 37
Filter	Opens the Capture/Filter application.	page 37
Capture	Opens the Capture/Filter application.	page 37

Launching an Ethernet RMON Utility

To launch an Ethernet RMON utility:

1. Double-click either an EtherMeter or Ethernet probe on the network map.
2. Click the RMON tab.
   The RMON tab window appears.



Ethernet RMON Utility Buttons

3. Click one of the RMON utility buttons to start the utility.
   For more information on a specific RMON utility, refer to the following sections.

RMON Statistics Window

The RMON Statistics feature evaluates the overall performance of a LAN segment. The Statistics window is frequently the first place to look if you suspect problems on the segment monitored by the meter.

Use the View menu to specify the view you want to display. The Statistics window can display different views of your network statistics:

- Errors View
- Packet Distribution View
- Packet Trend View
- Error Trend One View
- Error Trend Two View

Statistics - Errors View

The Errors table indicates the number of errors or events that occurred on the LAN segment to which the EtherMeter or Ethernet RMON agent is attached. The chart shows the number of errors of each type for the last polling interval.

When you choose View/Errors, MeterWare displays the following statistics:

- CRC Align

  Number of packets with a length from 64 to 1518 octets (excluding framing bits, including Frame Check Sequence [FCS] octets), but not an integral number of octets in length or with a bad FCS

- Collisions

  Shows when more than one device attempts to transmit data at a given time

- Undersize

  Number of packets less than 64 octets long (excluding framing bits, including FCS octets) that were otherwise well formed

- Oversize

  Number of packets longer than 1518 octets (excluding framing bits, including FCS octets) that were otherwise well formed

- Fragments

  Number of packets that were not an integral number of octets in length or that had a bad FCS and were less than 64 octets in length (excluding framing bits, including FCS octets)

- Jabbers

  Number of packets longer than 1518 octets (excluding framing bits, including FCS octets) and not an integral number of octets in length or that had a bad FCS

- Drop Events

  Total number of times (events) packets were dropped due to controller buffer overflow

Statistics - Packet Distribution View

When you choose View/Packet Distribution, MeterWare displays statistics for the LAN segment monitored by the EtherMeter or Ethernet RMON agent.

The Packet Distribution bar graph displays the number of packets of each size observed in the last sampling interval, including:

- Size 64

  Number of 64-byte packets

- Size 65 - 127

  Number of 64-byte to 127-byte packets

- Size 128 - 255

  Number of 128-byte to 255-byte packets

- Size 256 - 511

  Number of 256-byte to 511-byte packets

- Size 512 - 1023

  Number of 512-byte to 1023-byte packets

- Size 1024 - 1518

  Number of 1024-byte to 1518-byte packets

The table at the bottom displays delta for each packet size group and rates. The table also displays the delta % which is the mix in the last sample and cumulative % which is the percentage mix of packet sizes for the entire time that the statistics group has been running on the agent.

Statistics - Packet Trend View

When you choose View/Packet Trend, MeterWare displays statistics for the LAN segment monitored by the Ethernet RMON agent.

Statistical Trend displays threebar graphs which indicate:

- Packets per Second

  Number of packets/second on this network segment for each sampling interval

- Utilization Percent

  Utilization of this network segment, in a percent for each sampling interval

- Broadcast/Multicast Rate

  Total number of broadcasts and multicasts for each sampling interval

Statistics - Error Trend One View

When you choose View/Error Trend One, MeterWare displays error statistics for the LAN segment monitored.

Error Trend One displays threebar graphs which indicate:

- Kilo Octets/Second

  Shows network load for comparison of collisions and total errors shown on other twographs

- Collisions/Second

  Shows when more than one device attempts to transmit data at a given time

- Total Errors/Second

  Shows sum of all Ethernet errors on the segment

Statistics - Error Trend Two View

When you choose View/Error Trend Two, MeterWare displays error statistics for the LAN segment monitored.

Error Trend Two displays three bar graphs which indicate:

- CRC Alignment Errors/Second

  Indicates errors in the CRC field of the Ethernet frame

- Undersize and Oversize Errors/Second

  Undersize errors are for Ethernet frames with less than 64 bytes with a good CRC; oversize errors are for Ethernet frames with greater than 1518 bytes and have a good CRC

- Fragments and Jabbers Errors/Second

  Fragments are frames with less than 64 bytes and a bad CRC; jabbers are frames with greater than 1518 bytes and a bad CRC

RMON History Window

The RMON History window provides long-term historical views of network statistics.

MeterWare lets you take statistical samples of network traffic based on sampling intervals that you specify. You can define the number of buckets (for example, samples to save) and sampling interval. Sampling intervals may be from one second up to one hour.

Traffic observation samples offer insight into network performance trends and provide valuable information for network optimization and growth planning.

NOTE: Upon opening the RMON History window, if no history control entries have been created, you are prompted to add a control entry. See "Adding NND Control Table Entries."

When you have defined a history control entry, MeterWare displays two tables of history statistics for the specified control entry.

RMON Host Window Overview

The RMON Host window shows nodes on the LAN segment and the status of those nodes. It also allows you to observe the traffic statistics for all nodes monitored on the network segment.

When you open the Host window, it displays the RMON Host Table in a tabular format. Use the RMON Host window to evaluate what nodes are on your network, the active or inactive state of those nodes and which nodes may be causing problems.

Host Window Views

The Host window can display different views of your network statistics:

- Cumulative

  The total count of each type of traffic, from each host, since the Host table was created

- Delta

  The change in values since the last interval

RMON TopN Window Overview

The RMON Host TopN displays the stations generating the most traffic for a given parameter.

TopN organizes the presentation of the results in descending order. The first host in the sequence has the highest percentage for a given statistic. For example, if Out Broadcast is selected, the host sending the highest percentage of broadcast packets is listed at the top of the chart.

When you open the TopN window, it displays information in a pie chart and table format.

RMON Matrix Window Overview

The RMON Matrix maintains statistics for conversations between devices (hosts). It is an ideal way to analyze who is talking to whom on the network. It is also useful in isolating nodes that are sending out errors.

The RMON Matrix table displays the amount of traffic and the number of errors between an address pair (one source address and one destination address) on the network. For each address pair, statistics counters are maintained for the number of octets, packets and error packets between the addresses.

You can view the data in a cumulative or delta format. The Matrix table shows entries by name (if defined) or by MAC address. The table displays the entries in the order of source MAC address.

When you open the Matrix window, it displays the RMON Matrix Table in a statistical format. Use the View menu to specify the view you want to display.

- Cumulative

  The cumulative number of each RMON Matrix traffic statistic since the matrix table was created

- Delta

  The counts for the current sampling interval

RMON Alarm/Event Control Table Overview

The RMON Alarm feature takes statistical samples from variables in the agent and compares them to previously defined thresholds. If the monitored variable crosses a threshold, an alarm is generated. That alarm is automatically linked to the Event table by way of the index number.

The Alarm/Event window displays the current settings for alarms and events set-up on the agent. The RMON Event table processes alarms.

RMON Event Window Overview

The RMON Event table processes alarms, based on the parameters set in the Event table. You can set the Event table to discard the alarm, log the alarm for later review or provide notification by way of an SNMP trap message. Additionally, a DOS command may be launched from an event. Typically, the DOS command is a batch file; for example, a batch file might dial a beeper, send an e-mail or take a corrective action for a network problem.

The Event window displays two tables:

- Event Table
- Event Log Table

RMON Capture/Filter Overview

The RMON Capture/Filter application gives you powerful tools for troubleshooting network problems. You can now perform protocol analysis and decode individual packets remotely.

Capture/Filter decodes packet information down to the lowest data level. You define the filtering conditions and Capture/Filter sends your parameters to the RMON agent. The agent then returns all packets which meet the filter criteria back to MeterWare for decoding and additional analysis. Decoding allows you to obtain a detailed description of what is in each matched packet.

How to Access the Capture/Filter Window

To open the Capture/Filter application, do one of the following:

- Click Filter or Capture in the RMON tab after double-clicking an EtherMeter, Ethernet RMON agent, TokenMeter or Token Ring RMON agent on the Network Map.

The RMON Capture/Filter Window

The Capture/Filter window contains four tabs:

- The Channel tab lets you edit channel parameters, view the status of all channels and view applied filters
- The Filter tab lets you specify the filter criteria, including addresses and protocols, for the packets to be captured
- The Analyze tab lets you refine the packets in MeterWare's buffer through the use of powerful post-filters
- The Buffer tab displays packets as they are captured and provides protocol decodes

Channel Tab (Capture/Filter Application)

The Channel Tab lets you create channels, set up channels and run, stop and free channels. For information on using the Channel tab, see "Editing Channel Configuration."

Channel Tab Window Options

The information in the Channels Status screen area shows the following information for each channel:

- Channel

  Indicates the name of the channel

- Status

  Indicates whether this particular channel is running

  Running indicates the agent is capturing data

  Stopped indicates the agent is not capturing data (but memory may be allocated to it)

  Free indicates the channel is free and not using agent memory or CPU cycles

- Buffer Granted

  Shows how many bytes of the RMON agent's buffer are allocated to the channel. A value of max means all of the agent's memory resources are allocated to the packet capture function. If all of the agent's buffer has been allocated to a few channels, no additional channels can be created.

- Filters Attached

  Indicates the number filters applied to this channel.

- Packets in Buffer

  Indicates the number of captured packets that have been downloaded into MeterWare's buffer.

- Edit

  Displays the Edit Channel dialog box, where you specify configuration criteria for capturing and storing packet information for the selected channel. The most important parameter is Requested Buffer Size. If the agent has enough space in its buffer and can allocate the requested memory resources, it accepts the criteria and notifies you that the buffer has been granted.

  After a channel has been created, you cannot edit it until you choose Free.

- Refresh

  Polls the agent to obtain the latest status on all channels.

- Create/Attach

  Assigns resources in the RMON agent to the selected channel per the criteria specified in the Edit Channel dialog box. Once a channel has been created this button toggles and becomes the Attach button which can be used to apply pre-saved filter templates.

- Free

  Frees the channel and releases buffer memory in the agent.

- Run

- Begins capturing packets on this channel.

  If Lock is chosen for the Action on Full Buffer, when the number of captured packets reaches the requested buffer size, the packet capturing process stops and the Buffer Status reports Full.

  If Wrap is specified as the Action on Full Buffer, the number of captured packets in the buffer increment until the buffer reaches its maximum capacity. The number of captured packets begins to fluctuate, depending upon the buffer size and capture slice size.

- Stop

  Stops capturing packets on this channel.

NOTE: Double-click the meter icon next to each channel to display filters applied to that channel. Double-click a channel row to display the Edit Channel dialog box.

Filter Tab (Capture/Filter Application)

The Filter Tab lets you specify the source and destination address for the packets to capture.

Filter Tab Window Options

- Link Layer

  Specifies the link layer encapsulation type.

- Protocol

  Specifies the protocol for which to capture packets. Some of the protocols supported by MeterWare include:

  TCP/IP

  Novell IPX/SPX

  DECnet

  AppleTalk

  XNS

- Sub-Protocol

  Specify the sub-protocol for which to capture packets.

- Source Address

  Specifies the source address for the packets. Specify the address and whether it is a Protocol Address or a MAC Address.

- Destination Address

  Specifies the destination address for the packets. Specify the address and whether it is a Protocol Address or a MAC Address.

- Allow Packets:

  Specifies the allowed packet type(s) to be accepted in the current filter.

- DATA/MASK/NOT:

  Slide control that determines which filter information is displayed in the Filter Pattern Field window.

- Filter Pattern Field window:

  This window displays in hex format either the data pattern, mask or logical NOT mask pattern for the current filter as selected by the

DATA/MASK/NOT selector control.

- <-- x of n --> :

  Allows user to select filter x out of n total filter templates for the current channel. If more than one template exists for the current channel (i.e., n> 1) then yellow arrows will appear which can be used to select among the filter templates. Click on the yellow arrow pointing to the right to select a higher number filter template or click the left arrow to select a lower numbered filter.

- Create:

  Creates a new filter template which may be configured and then applied to the current channel.

- Apply:

  Applies the current filter template to the current channel.

- Run/Stop Toggle:

  Begins or stops the capturing of packets.

  If Lock is chosen for the Action on Full Buffer, when the number of captured packets reaches the requested buffer size, the packet capturing process stops and the Buffer Status reports Full.

  If Wrap is specified as the Action on Full Buffer, the number of captured packets in the buffer increment until the buffer reaches its maximum capacity. The number of captured packets begins to fluctuate, depending upon the buffer size and capture slice size.

Analyze Tab (Capture/Filter Application)

The Analyze Tab lets you refine the packets already captured in the buffer tab window:

To analyze a channel:

1. Click the Analyze tab. (Note: If you plan to use the Data Function in an expression, first select a packet in the Buffer tab before going to the Analyze tab.)
2. Build an expression by choosing the Protocol or Data Function controls in the Analyze tab.
3. Select the link encapsulation type from the lower list box.

4. Select the appropriate higher layer protocol information from the middle list box. Click the Add button for each selection you make in the middle list box. You will see the expression being built in the upper list box.
5. When this term of your expression is complete click the check button at the right of the box to move this term of the expression to the large Expression box at the upper left corner of this tab page.
6. You may now apply this analyze expression to the current buffer contents or continue to build a more complex expression by inserting a logical AND or OR via keys on the calculator keypad and then selecting Protocol or Data to create a new term.

Saving Expressions

Use the File/Save As option to name and save any analyze expressions that you want to reuse in the future.

Analyze Tab Window Options

- Expression

  Displays the current expression as it is created term by term. This is the post-filter that will be applied to the buffer contents when the apply button is used.

- Apply

  Applies the current expression filter to the current buffer contents and switches view to the Buffer tab.

- Source Address/Destination Address

  Lets you filter packets you have already captured based on the source and/or destination MAC or protocol addresses.

- Calculator Keypad

  Lets you enter numbers and operators into the expression.

  CE Clears the last entry.

  C Clears all fields except Data Offset.

- Protocol Function

  Click to create a post-filter term based on protocols.

- Data Function

  Allows you to create a post-filter term based on protocols. Displays raw data for the packet selected in the Buffer tab. You can select a portion of the packet by selecting it from the Raw Data window.

- Link Layer Encapsulation Selection Box

  Allows you to select the link layer encapsulation.

- Higher Layer Protocol Selection Box

  Allows you to select higher layer protocols.

- Raw Data

  Shows a hex dump of the currently selected packet. This field is used when selecting the data pattern to be used with the Data Function control.

NOTE: Use the "!" character before an expression to yield the logical NOT of the expression.

Buffer Tab (Capture/Filter Application)

Displays packets as they are captured. The display is continuously updated until you stop the capture or click the stop light in the buffer tab to pause downloading of captured packets.

Buffer Tab Window Options

The Buffer tab has three windows that you can resize by dragging the separator bars.

Top Window

Displays summary information on each packet. The summary table contains the following fields:

- Index

  The index number of the captured packet as assigned by the RMON agent.

- Length

  The length of the captured packet in bytes (octets).

- Time stamp

  The time the packet was captured by the RMON agent. The time stamp is controlled through the pull down Options menu. The time stamp field may be selected via the Options/Time Stamp Format menu:

- Absolute Timestamp displays the clock time the packet was captured

- Relative Timestamp displays the time the packet was captured relative to the time the first packet was captured

- Interpacket Timestamp displays the time the packet was captured relative to the time the previous packet was captured. The timestamp resolution is 100 milliseconds.

- Source

  The source address of the captured packet

- Destination

  The destination address of the captured packet

- Protocol Type

  The protocol type of the captured packet or the value of the packet in offset 12.

  The display is continuously updated until the Capture/Filter application retrieves all of the information from the buffer.

- If you specified Lock as the Full Action, the application stops uploading new information when the buffer is full.

- If you specified Wrap as the Full Action, the display updates continuously.

Buffer Tab Middle Window

Decodes protocols for each ISO layer for the selected packet.

When you click a field in the middle window, the corresponding area in the bottom window is highlighted.

NOTE: If the length of the packet is greater than the Download Slice Size as set in the Edit Channel options then a "Bad Checksum protocol error" message may appear in the decode window since the checksum is being calculated on an incomplete packet download.

Buffer Tab Bottom Window

Displays the selected packet in raw hexadecimal dump format.

NOTE: Use the Options/Polling Interval dialog box to control the polling and downloading of packets from the RMON agent to the buffer window in MeterWare. Use the Options/Tear-off Record to take a snapshot of the current packet trace and save it in a new independent window. This is very useful when comparing and analyzing multiple traces.

Steps for Establishing a Basic Capture/Filter

1. Start the Capture/Filter application.

   For more information, click the RMON Capture/Filter Overview topic.

2. From the Channel tab, select a Free channel then click the Create button.

   For more information, click the Editing Channel Configuration topic.

3. From the Filter tab, specify the source address, destination address, protocol or pattern for the packets to be captured.
4. Click the Apply button then click the Run button.
5. In the Buffer tab, view the captured packets and protocol decodes.
6. In the Analyze tab, refine the packets you have captured.

Editing Channel Configuration

To edit a channel's configuration:

1. Select a channel row for which the status is Free.
2. Click Edit (or double-click a channel row entry).

   The Edit Channel dialog box is displayed.

3. Enter the following information in the Edit Channel dialog box:
   - Channel Name: Names the filter group.
   - Filter Criteria: Accept specifies that all packets matching the channel's filter criteria are loaded into the buffer. Reject specifies that all packets except those matching the channel's filter criteria are loaded into the buffer.
   - Action on Full Buffer: Specifies what the RMON agent does when its packet capture buffer is full. Lock means the packet capturing process stops when the RMON agent's buffer is full. Wrap means the packet buffer is continually reused. As the new matched packets are collected, the oldest packets are deleted.
   - Packets: Provides details about the number of bytes of each packet to capture into agent memory and specify the number of bytes for each packet to transfer to MeteWare for analysis.

     Capture Slice Size specifies the portion (number of bytes) of each matched packet to be stored in the agent's buffer. If you request a smaller capture size, more packets can be stored in the agent's buffer. See Capture Slice & Download Sizes.

     Download Slice Size specifies how many bytes of each captured packet is sent to the managing application (i.e., MeterWare) when packets are retrieved. See Capture Slice & Download Sizes.
   - Requested Buffer Size: The amount of memory to allocate for storing the captured packets. The default value is 15KB. See Requested Buffer Sizes.
4. Click either OK to return to the Channel tab or Create to create the channel.

   If the Create request is unsuccessful, it may be because you do not have Read_Write access to the RMON agent, the agent does not have enough resources or both. If the channel is successfully created, the Resource Created column displays Stopped or Running status.

Viewing the RMON Filters, Channels and Buffers

The RMON tables show you the RMON filters, channels and buffers created on the currently selected RMON agent.

To view the RMON tables:

1. Choose Window/RMON Tables from any tab in the filter/capture applet.

   The RMON Tables dialog box is displayed, with the following tabs. Each tab shows an RMON table:

   - RMON Channels provides detailed information regarding RMON channel configuration
   - RMON Filters provides detailed information regarding RMON filter configuration
   - RMON Buffers provides detailed information regarding RMON buffer configuration

2. Select a row in any of the tabs and then either double-click it or select View Details.

Saving a Buffer and Viewing a Saved Trace File

All of the packets received by the Capture/Filter application for a particular buffer can be saved to a file. Once packet information has been saved, it can be viewed at any time.

To save a buffer:

1. From the Buffer Tab Choose File/Save As... or the disk icon from the tool bar.
2. Enter a description of the trace or accept the default as shown.
3. Enter path and name of trace file then save with .trc as file type. Click OK.

Viewing a Saved Trace File

To view a saved trace file:

1. From the Buffer Tab Choose File/Open or the folder icon from the tool bar.
2. Specify the *.trc file to be loaded into the buffer.

   The Trace Description field appears in the lower left corner of the Open Trace dialog box.

Types of Filter Packets Allowed

The packet types are the following:

- Any Packets

  Capture all packets.

- No Errors

  Capture only good packets.

- Any Errors

  Capture all packets with any type of error.

- Fragment

  Capture all packets that are less than 64 Octets and that have a CRC/Alignment error.

- Jabber

  Capture all packets that are greater than 1518 Octets and that have a CRC/Alignment error.

- CRC/Align

  Capture all packets with CRC/alignment errors detected in the FCS (frame check sequence).

- Short

  Capture all packets with less than 64 bytes with or without CRC/ Alignment errors (i.e., capture fragments AND undersize frames).

- Undersize

  Capture all packets that are less than 64 Octets and DON'T have a CRC/Alignment error.

- Long

  Capture all packets greater than 1518 bytes with or without CRC/ Alignment errors (i.e., capture jabbers AND oversize frames).

- Oversize

  Capture all packets that are greater than 1518 Octets and DON'T have a CRC/Alignment error.

- After Drop

  Capture all packets after one or more packets were dropped by the RMON agent.

- Frame Copied

  Capture all packets with the Frame Copied bit set in the Token Ring frame header.

- Address Recognized

  Capture all packets with the Address Recognized bit set in the Token Ring frame header.

- Other

  Capture all packets with status other than (i.e., not including) the above error conditions.

Editing Channel Configuration

To edit a channel's configuration:

1. Click a test channel row for which the status is Free.
2. Click Edit (or double-click a channel row entry).

   The Edit Channel dialog box is displayed.
3. Enter the following information in the Edit Channel dialog box:
   - Channel Name: Names the filter group.
   - Filter Criteria: Accept specifies that all packets matching the Address pattern and the filter criteria are loaded into the buffer. Reject specifies that all packets except those matching the Address pattern and filter criteria are loaded into the buffer.
   - Action on Full Buffer: Specifies what the RMON agent does when its packet capture buffer is full. Lock means the packet capturing process stops when the RMON agent's buffer is full. Wrap means the packet capturing process wraps when the agent's buffer is full. As the new matched packets are collected, the oldest packets are deleted.

   - Packets: Provides details about number of bytes of each packet to capture into agent memory and specify the number of bytes for each packet to transfer to MeterWare for analysis.

     Capture Slice Size specifies the portion (number of bytes) of each matched packet stored in the agent's buffer. If you request a smaller capture size, more packets can be stored in the agent's buffer. See Capture Slice & Download Sizes.

     Download Slice Size specifies what portion of each captured packet is retrieved. See Capture Slice & Download Sizes.

   - Requested Buffer Size: The amount of agent memory to allocate for storing the captured packets. The default value is 15KB. See Requested Buffer Sizes.
4. Click either OK to return to the Setup tab or Create to create the channel.
5. Choose Options/Polling Interval to specify how often MeterWare polls the agent to check for packets. Specify the time in seconds, from 1 to 32767. Also, specify the number of packets to retrieve for each polling interval.

Creating a Channel

To create a test channel:

1. Click a test channel row for which the status is Free.
2. Do one of the following:
   - Click Edit. Then, in the Edit Channel dialog box, edit the channel and click Create.
   - Click Create.

   If the Create request is unsuccessful, it may be because you do not have Read_Write access to the RMON agent, the agent does not have enough resources or both. If the test channel is successfully created, the Resource Created column displays stopped or running status.

Freeing Memory Resources

Once a test channel is created, you cannot modify it by clicking Edit until you free the resource.

To free a test channel:

1. Select the channel on the Setup tab.
2. Click Free.

   The memory area in the RMON agent is released.

Viewing the RMON Filters, Channels and Buffers

The RMON tables show you the RMON filters, channels and buffers created on the currently selected RMON agent.

To view the RMON tables:

1. Open the Setup tab.
2. Choose Window/RMON Tables.

   The RMON Tables dialog box is displayed, with the following tabs. Each tab shows an RMON table:

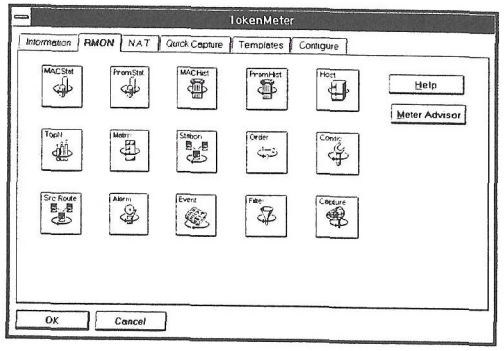
   - RMON Channels
   - RMON Filters
   - RMON Buffers

Launching a Token Ring RMON Utility

To launch a Token Ring RMON utility, do the following:

1. Double-click a TokenMeter or Token Ring probe on the network map.
2. Click the RMON tab.

   The Token Ring RMON tab appears.



3. Click an RMON utility button to start the utility.

   Refer to the following following sections for more information on a Token Ring utility.

MAC-Layer Statistics Overview

The MAC-layer Statistics application displays real-time statistics on normal, repeat-mode activity. These errors and statistics are specific to the Token Ring protocol and are used to manage the flow of traffic on the ring.

The window displays different views of MAC-layer Token Ring statistics. Each view includes a graph and corresponding table.

Use the View menu to choose from among the three different views of MAC-layer statistics:

- Events
- Errors
- Packets

These views are described in more detail in the following sections.

MAC-Layer Stats - Events View

When you choose View/Events, MeterWare displays a graph of the delta values for six Token Ring event statistics. A tabular display below the graph gives additional rate, Delta % and Cumulative % information.

A description of each event statistic is given below.

- NAUN Changes

  The number of Nearest Active Upstream Neighbor (NAUN) changes detected by the TokenMeter. NAUN changes occur when a new station enters the ring or the current NAUN takes itself off the ring.

- Ring Poll

  The Active Monitor (AM) initiates the Ring Poll process every 7 seconds. In this way, stations are kept aware of their NAUNs and that the ring is functioning properly. The Ring Polls number indicates the number of ring polls initiated by the Active Monitor.

- Ring Purge

  The Active Monitor uses the Ring Purge process to restart the ring after a break in the token protocol. The Ring Purge statistic is the number of times the ring goes from a normal ring state into a Ring Purge state. (This statistic excludes any ring purge states that occur as a result of beacon or claim token states.)

- Claim Token

  The Claim Token events statistic indicates the number of times the ring has gone into the claim token process. Token claiming (often referred to as monitor contention) is the process during which stations go into contention to win the Active Monitor role.

- Beacon

  The Beacon events statistic indicates the number of times the ring goes into a beaconing state. A beaconing state occurs when a ring station detects a hardware error on the ring and generates a beacon frame. Token Ring defines 4 error levels. The beaconing state is at the highest (or most severe) error level.

- Drop

  The Drop events statistic indicates the number of times the probe detected a lack of resources and hence may have missed counting some packets.

MAC-Layer Stats - Error Window

When you choose View/Errors, MeterWare displays two error statistics graphs. Tabular displays below the graphs give additional Delta, Delta % and Cumulative % information.

A description of each error statistic is given below.

- Lost

  An originating station reports a Lost Frame when it transmits a frame onto the ring and doesn't get it back.

- Abort

  A ring station reports an Abort Delimiter error when, while transmitting a frame, it encounters a recoverable internal error. After transmitting an Abort error, the ring station does not transmit a token.

- Address Copied (AC)

  When a station reports an Address Copied Error (ACE), it indicates a problem with the reporting station's upstream neighbor. The reporting station's upstream neighbor couldn't properly set the frame copies or address recognized bits in the newly sent frame, even though it successfully copied the bits on the last frame it received.

- Burst

  A reporting ring station generates a Burst error when it detects a signal error in the Token Ring cabling medium. Usually, Burst errors are a result of a station entering or leaving the ring.

- Internal

  An Internal error occurs when a ring station's adapter detects a minor recoverable error in its hardware.

- Line

  The TokenMeter reports a Line error when it detects a packet which is not an integral number of octets in length or has a bad FCS (Frame Check Sequence).

- Soft

  This statistic indicates all Soft errors discovered on this segment by the probe. Soft errors are the least severe of the Token Ring errors. Soft errors only temporarily disrupt normal ring operations.

- Token

  When the token is not detected on the ring, the Active Monitor reports a Token error. Only the Active Monitor generates a Token error.

- Frequency

  A Frequency error occurs when the reporting ring station attempts to receive a frame from its NAUN that does not contain the proper ring-clock frequency.

- Frame Copied

  A ring station reports a Frame Copied error when it believes another station may have the same address as its own – a duplicate address.

- Congestion

  A Congestion error occurs when a station receives a frame, but doesn't have the buffer space to store it.

MAC-Layer Stats - Packet View

When you choose View/Packets, MeterWare displays a packet/octet distribution graph. This allows you to see exactly what processes are occurring to initialize and maintain operation of the Token Ring IEEE 802.5 protocol. A tabular display below the graph gives additional Delta, Rate, Delta % and Cumulative % information.

A description of each packet statistic is given below.

- Octets

  The total number of octets of data in MAC packets (excluding those that were not in good frames) received on the network (excluding framing bits but including FCS octets).

- MAC

  Media Access Control (MAC) Packets carry Token Ring management information and are specific to a ring. Ring stations use MAC packets to maintain token protocol on the ring. Token Ring has 25 MAC packet types, which provide insight into the low-level packet communication processes.

- Ring Purge

  The Active Monitor generates a Ring Purge MAC packet when it has to restart the ring after a break in the token protocol.

- Beacon

  The total number of Beacon MAC packets detected by the probe. When a station detects a hardware error on the ring, it generates a beacon packet. Token Ring defines 4 error levels. The beaconing state is at the highest (or most severe) error level.

- Claim Token

  The number of Claim Token packets detected by the probe. The Claim Token statistic indicates the number of times the ring has gone into the claim token process. Token claiming (often referred to as monitor contention) is the process during which stations go into contention to win the Active Monitor role.

Promiscuous Statistics Window

The Promiscuous Statistics window displays real-time utilization statistics on normal data packets.

MAC-Layer History Window

The MAC-Layer History window displays historical MAC-Layer utilization and error statistics. Statistics include error reports for the ring and ring utilization of the MAC-Layer.

MeterWare lets you take statistical samples of network traffic based on sampling intervals that you specify. You can define the number of buckets (samples) and sample intervals of up to 60 minutes.

Traffic observation samples offer insight into network performance trends and provide valuable information for network optimization and growth planning.

Promiscuous History Window

The Promiscuous History window displays trend statistics from data packets collected promiscuously. The statistics shown include broadcasts, multicasts, octets, drop events and packet sizes.

MeterWare lets you take statistical samples of network traffic based on sampling intervals that you specify. You can define the number of buckets (samples) and bucket intervals of up to 60 minutes.

Traffic observation samples offer insight into network performance trends and provide valuable information for network optimization and growth planning.

Ring Station Window

The Ring Station window shows a table of statistics and status information associated with each Token ring station on the local ring. This application is useful in analyzing the relationships between events on the ring. Certain patterns of behavior by ring stations can uncover possible trouble areas.

For example, a disruption occurs on the ring every time a station inserts itself. This in turn causes a ring purge event and issuance of a new token by the active monitor. You can use the ring station tool to identify who the inserting nodes are, as well as who the active monitor is. The Ring Station application enables you to:

- Pinpoint isolating and non-isolating errors
- Identify active and inactive stations
- View patterns of network activity

Station Order Window

The Ring Station Order window displays up-to-date Token Ring status information including the order of stations on the monitored ring, which ring you are monitoring, how many active stations there are, who the beacon sender is and so on.

Station Configuration Window

The Station Configuration window actively manages Token Ring stations. The Configuration tool allows you to retrieve configuration information from individual stations.

Source Routing Window

The Source Routing window displays utilization statistics derived from source routing information present in Token Ring packets in a source route bridging environment.

Source routing bridges operate at the data link-layer and connect multiple rings into a single logical network. Source route bridges forward frames based on the route information contained in the RIF (routing information field).

Chapter 4 N.A.T. Extensions

N.A.T. has extended the RMON MIB functionality with the definition of N.A.T.-specific meter management applications. These applications include the following:

- New Node Discovery
- IP Mapping
- Peak
- Top 10
- Zoom
- Protocols

Accessing N.A.T.-specific applications

To access the N.A.T.-specific applications,

1. Double-click an EtherMeter or TokenMeter on the Network Map.
   MeterWare displays the Information tab of the Meter dialog box.
2. Choose the N.A.T. tab.
3. Choose the N.A.T.-specific application you want to access.
   For more information on a specific N.A.T. application, refer to the following sections.

New Node Discovery Window

New Node Discovery (NND) assists you in providing network security by monitoring the network for nodes not in the host table. The NND builds an initial table based on the Host Table. Once the NND Table is established, you can add devices known to be legal or delete entries suspected of being illegal to see if they reoccur. If a node is discovered, New Node Discovery can log the discovery or, optionally, send a trap.

If no NND control entries have been created, you are prompted to add a control entry. See Adding NND Control Entries.

NND Table

The NND window displays the following:

- Index Number
- Address
- Order

The number of new nodes detected is displayed at the bottom of the NND Table window.

Adding NND Control Entries

The NND Control Table window allows you to add NND control entries. If no NND control entries have been created, the NND Control Table automatically appears on your screen when you launch the application. To access the Control Table from the main NND menu, choose Control Tables from the Table menu.

To add a control entry, do the following:

1. Choose Add.
   The New Node Detection Control Table appears.
2. Enter a new index number or accept the default.
3. Enter a new host number or accept the default.
4. Specify the trap sending mode by choosing the applicable radio button (Enable or Disable).
5. Choose Get Host Table to retrieve all of your host table addresses.
6. Choose Add to add an additional address. At the Address Input screen, select or enter the MAC Address you want to add to the table and choose OK.
   -or-
   Select an address and choose Delete to remove the unwanted addresses from your host table. Choose OK.
7. Choose OK when you are finished with the NND Control Table.
   Your newly created entry appears in the NND Control Table.
8. Select the newly created entry and choose View to view any newly discovered nodes.
   -or-
   Choose Close to close the NND Control Table window.

NND Control Table Variables

A description of each NND Control Table column variable is given below:

- Index: The control index is a randomly generated number used internally by the system. It uniquely identifies an entry in the Control Table. You can change the Control Index displayed on the New Node Detection Control Table by typing over the existing data.
- Host : If the meter supports multiple host tables (e.g., EtherMeter/450), the host index allows you to differentiate between those tables. You can change the Host Index displayed on the New Node Detection Control Table by typing over the existing data.
- Trap: You can log a trap by selecting Enable. Choose Disable if you don't want to log traps.
- Mode: A value of 1 in the Mode column indicates the NND table is set to match the RMON Host Table information. If a new node is subsequently added, the system detects its presence. A value of 2 means the system stops learning new nodes but still updates the statistics for existent host entries.
- Freeze Size: The size of the RMON Host Table to freeze.
- NND Size: The number of host entries in the NND Host Table. These entries also exist in the associated RMON Host table, but are considered illegal hosts since they are learned after the RMON Host Table is frozen.
- Up Time: The time the NND table was last set to match the frozen RMON Host Table information.
- Status: A value of 1 indicates the NND function is enabled. A value of 4 indicates the NND function is disabled. Other values result in a "badValue" error message.

Modifying NND Control Entries

The NND Control Table window allows you to modify NND control entries. To access the NND Control Table from the main NND menu, choose Control Tables from the Table menu.

To modify a control entry, do the following:

1. Double-click on an entry in the Control Table or highlight an entry and click Modify.

   The New Node Detection Control Table appears.

2. Modify one or more of the following:
   - Index
   - Host
   - Trap Sending Mode
3. Choose Get Host Table to retrieve all of your host table addresses.
4. Choose Add to add an additional address. At the Address Input screen, select or enter the MAC Address you want to add to the table and choose OK.

   -or-

   Select an address and choose Delete to remove the unwanted addresses from your host table. Choose OK.
5. Choose OK when you are finished with the NND Control Table.

   Your modified created entry appears in the Control Table.
6. Select a control entry and choose View to view any newly discovered nodes associated with that entry.

   -or-

   Choose Close to close the Control Table window.

IP Mapping

IP Mapping matches the MAC address with the IP address. IP Mapping also detects multiple (duplicate) IP addresses for a single Ethernet address and changed IP addresses. This helps to avert potential conflicts between addresses and detect unauthorized changes in IP addresses.

IP Mapping Table

The IP Mapping window displays the following:

- MAC Address
- IP Address

To reset or disable the IP Mapping Table, choose the applicable command from the Table menu.

Adding IP Mapping Control Entries (EtherMeter Only)

The IP Mapping Control Table window allows you to add IP Mapping control entries. If no IP control entries have been previously created, the IP Mapping Control Table automatically appears on your screen when you launch the application. To access the Control Table from the main IP Mapping menu, choose Control Tables from the Table menu.

To add a control entry, do the following:

1. Choose Add.

   The IP Mapping Control Entry window appears.
2. Enter a new index number or accept the default.
3. Enter a new host number or accept the default.
4. Specify the trap sending mode by choosing the applicable radio button (Enable or Disable).
5. Choose Add to add an address(es) to the Router Table. At the Address Input screen, select or enter the router's MAC address you want to add to the table and choose OK.

   -or-

   Select an address and choose Delete to remove the unwanted address from your router table. Choose OK.

NOTE: With Trap enabled, failure to list routers in the Router table may result in an excessive number of traps when the system detects duplicate IP addresses. This "Trap Storm" may adversely affect network performance. (See Adding Addresses to the Router Table for more information.)

6. Choose OK when you are finished with the IP Mapping Control Entry window.

   Your newly created entry appears in the NND Control Table.
7. Select the newly created entry and choose View to view the new IP Mapping table.

   -or-

   Choose Close to close the IP Mapping Control Entry window.

Adding Addresses to the Router Table (EtherMeter Only)

You can add addresses to or delete them from the IP Mapping table. Without the ability to delete Ethernet addresses from the IP Mapping table, routers would present a problem because they forward packets using the host IP address and their own Ethernet address. As a result, the system would detect routed packets as changed Ethernet addresses or duplicated IP addresses.

However, routers (and any other device you would like to shield from IP mapping) can be listed in the router table. Addresses listed in the router table are not displayed on the IP Mapping window. Adding an address to the router table reduces the chances of a router loop.

To add an Ethernet address, IP address or device name,

1. Click the Add button to display the Address Input Type window.
2. Click the desired Input Method.
3. Type the address in the Ethernet Address/IP Address/Device text box and click OK.
4. Click OK. The table is restarted and you are returned to the IP Mapping window. The list reflects the filter(s) you entered in the Ethernet Address Input window.

   To remove an address from the router table, click the address to be removed and click Delete.

Modifying IP Mapping Entries (EtherMeter Only)

The NND Control Table window allows you to modify NND control entries. To access the NND Control Table from the main NND menu, choose Control Tables from the Table menu.

To modify a control entry, do the following:

1. Double-click on an entry in the Control Table.

   The New Node Detection Control Table appears.

2. Modify one or more of the following:
   - Index
   - Host
   - Trap Sending Mode

3. Choose Add to add an address(es) to the router table. At the Address Input screen, select or enter the router's MAC address you want to add to the table and choose OK.

   -or-

   Select an address and choose Delete to remove the unwanted address from your router table. Choose OK.

   NOTE: With Trap enabled, failure to list routers in the router table may result in an excessive number of traps when the system detects duplicate IP addresses. This "Trap Storm" may adversely affect network performance. (See Adding Addresses to the Router Table for more information.)

4. Choose OK when you are finished with the IP Mapping Control Entry window.

5. Select a control entry and choose View to view the IP Mapping table.

   -or-

   Choose Close to close the IP Mapping Control Entry window.

IP Mapping Control Table Variables

A description of each IP Mapping Control Table column variable is given below:

- Index: The control index is a randomly generated number used internally by the system. It uniquely identifies an entry in the Control Table. You can change the Control Index displayed on the IP Mapping Control Entry window by typing over the existing data.
- Host: The host table on which the Ethernet to IP address mapping table will be based. If the meter supports multiple host tables (e.g., EtherMeter/450), the host index allows you to differentiate between those tables. You can change the Host Index displayed on the IP Mapping Control Entry window by typing over the existing data.
- Trap: If Enable is selected, traps are generated when a duplicate IP address or an IP address change is detected. If Disable is selected, trap sending is disabled.
- Table Size: The total number of entries in the table.
- Changed: The number of IP address changes detected.
- Dup: The number of duplicate IP addresses detected.
- Up Time: The time the IP Mapping table has been operational.
- Status: A value of 1 in the Status column indicates that the MAC Address to IP address mapping function is enabled. A value of 4 indicates the IP mapping function is disabled. Other values return a "badValue" error message.

Peak Statistics

The N.A.T. Peaks window displays a variety of peak statistics for frames, utilization, kilobytes, multicasts and errors.

Top 10 Window (EtherMeter Only)

The Top 10 window displays the top 10 station addresses for a user-selected category. To select a rate base category, choose View.

Additional information on the Top 10 window includes:

- Valid Entries
- Total Entries
- Threshold Value
- Sample Time
- Total Packets/Interval
- Matched Packets

Selecting a Top 10 Category

The Top 10 menu on the Top 10 window lets you select the type of devices you want included in the Top 10 count. You can choose from seven categories of Top 10 selection criteria, based on Ethernet address or IP address:

1. Choose View.
2. Choose from among the following categories:
   - Ethernet Talkers
   - IP Talkers
   - Ethernet Listeners
   - IP Listeners
   - Ethernet Pairs
   - IP Pairs
   - Ethernet Broadcasters

Zoom View

In addition to viewing three Zoom tables (Tabular view), you can view the health of your network segment in graphical format. The Zoom graphical format displays a real-time plot of the utilization, packet rate and for Ethernet errors (and for Token Ring data rate) for the LAN segment monitored. Rates for all packets, broadcast packets, multicast packets and errors are individually plotted. To view Zoom graphs, choose Graphical from the View menu. Real-time information displays for the following three graph types:

- Packet Trend
- Utilization
- Errors per second or Data Rate

Use the View menu to specify the view you want to display.

Protocols

There are different protocol utilities, depending upon your network.

Token Ring Protocols

The protocols window provides a tabular listing of the top Network Layer protocols in use on this ring. The information includes packets per second, octets per second and percentage of total traffic statistics.

This list also appears in a bar chart format. The table shows packets/second, octets/second and % of packets for each protocol type. The bar chart graphs in descending order by number of packets with top 10 protocols.

Ethernet Protocols Window Overview

The Protocol table displays up to 30 Ethernet protocol types in descending order of frequency. E-Types are found in the Ethernet Standard and the IEEE 802.3/ SNAP standard. The protocol table has the absolute count and percentage of overall traffic based on the number of good packets. The table of E-Types includes definitions for all of the commonly used Ethernet protocols.

Chapter 5 SNMP Tools

This chapter discusses the following SNMP Tools:

TOOL	DESCRIPTION	REFER TO...
SNMP Templates	Allows you to view user-defined groups of MIB variables for any SNMP device on the network.	page 74
SNMP Template Editor	Allows users to create their own SNMP templates	page 78
SNMP Utility	For use with SNMP managed devices, including other vendor's SNMP devices, the tool allows you to interactively view and change management information on SNMP managed devices on the network.	page 88
MIB Compiler	Allows you to compile MIB text files supplied by N.A.T. or other vendors, without leaving MeterWare. The MIBs become part of the MIB tree and can be accessed through the SNMP Utility and SNMP DA.	page 98
Learn	Allows you to learn the lates names, MAC address, and IP address of devices on the network.	page 106
Name Editor	Allows you to manage Name tables containing numeric values and corresponding text strings that are substituted in many MeterWare windows.	page 108

SNMP Templates

SNMP templates allow you to view user-defined groups of MIB variables for any SNMP device on the network. The user-defined groups of MIB variables are described in SNMP templates. N.A.T. provides you with a set of pre-defined templates or you can build your own library of SNMP MIB variable templates. Each template supports up to 30 MIB variables and five tables.

SNMP templates are available for both N.A.T.- and non N.A.T.-managed devices. The SNMP device must support the SNMP variables defined in the template for SNMP SET, GET and GET-NEXT operations to be successful.

To access the SNMP template application, complete the following procedures:

1. Double-click a meter on the Network Map.

   MeterWare displays the Information tab of the device dialog box.

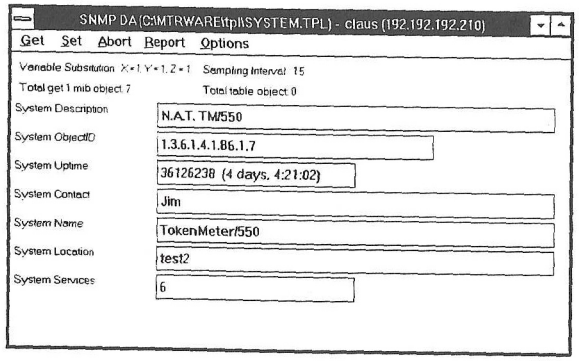
2. Click the Templates tab.

   A listing of defined templates appears. (Defined templates are stored in the MTRWARE\TPL directory).

3. Select and template and click View (e.g., SYSTEM.TPL).

   The SNMP DA window for the system template appears. See Figure 5-1.

Figure 5-1 SNMP System Template



The System template contains seven MIB variables. The template automatically fills in the MIB variables. If tables are defined in the template, you must click Get to retrieve the MIB information.

GET and SET Commands

The Get menu option performs an SNMP GET operation and updates the template. To perform a GET, simply click Get on the menu bar. All the MIB variables are updated.

The Set menu option performs an SNMP SET operation on a MIB variable. To use Set, click the MIB variable, modify it and click Set.

For example, in the System template, you could click the System Contact box, modify its contents and click Set. If the SET is successful, a "Set Operation Successful" message appears. If the SET fails, a "Operation Failed" message appears. A blank field in the template may indicate that the device does not support the MIB variable.

SNMP DA Options

The following options are available on the SNMP DA Options menu.

COMMAND	DESCRIPTION
Sampling Interval	Enters a sampling interval measured in seconds.
Disable Request	Stops the periodic updating of MIB information. Click Disable Request to toggle the feature. This can be useful when you are performing SET operations and you want to temporarily stop the information updates. A check mark next to Disable Request indicates periodic updating of MIB information has been stopped. No check mark indicates periodic updating of MIB information is being performed
Request in Multiple Packets	Indicates SNMP GET requests are issued until all MIB variables in the template have a value. No check mark (inactive) next to Request in Multiple Packets indicates only one GET per MIB variable is issued. If a MIB variable in the template is not found, no further attempts are made. If the Request in Multiple Packets feature is active, the system continues to issue GETs until every MIB variable has a value. Once a MIB variable has a value, the system stops issuing GETs for that variable. Click Request in Multiple Packets to toggle the feature.

Pre-Defined SNMP Templates

N.A.T. provides pre-defined SNMP standard and device dependent templates. Standard templates contain MIB variables from the standard SNMP groups system, interface, IP, snmp, icmp and udp. The file names are listed and described below:

system.tpl	System group MIBs
interfac.tpl	Interface group MIBs
ip.tpl	MIB-1 IP group MIBs
ip2.tpl	MIB-2 IP group MIBs
snmp_in.tpl	SNMP group In statistics
snmp_out.tpl	SNMP group Out statistics
icmp_in.tpl	ICMP group In statistics
icmp_out.tpl	ICMP group Out statistics
udp.tpl	UDP group MIBs

RMON Templates

RMON templates contain MIB variables from the RMON group. The RMON template files are listed and described below:

topn88.tpl	For creating and viewing the Host TopN table using an index of 88
filt100.tpl	For creating and viewing the filter and channel table using an index of 100
capt100.tpl	For creating and viewing the buffer table using an index of 100
rmonchk.tpl	For viewing how many tables exist in the following groups: statistics, host, matrix, alarm and event
rmonchk2.tpl	For viewing how many tables exist in the following groups: history, host TopN, filter and capture

N.A.T. Enterprise Templates

N.A.T. Enterprise (device dependent) templates contain MIB variables from the N.A.T. enterprise-specific group. The template files are listed and described below:

ILC/200 AND ILC/250	
ilc.tpl	For viewing port auto-partition and administrative states and resetting port statistics
LANB/155 AND LANB/250	
peak.tpl	For viewing peak segment statistics
LANB/100M, LANB/200M, ILC/200 AND LANB/290 (WITH BRIDGING)	
brdglan.tpl	For setting flush variables and doing a LAN table dump
LANB/290	
routfilt.tpl	For viewing the filter table
routstge.tpl	For setting a generic filter on entry 1 of interface 1
routstpo.tpl	For setting a IP filter on entry 1 of interface 1

The templates are located on your MeterWare utility diskette in the TPL subdirectory.

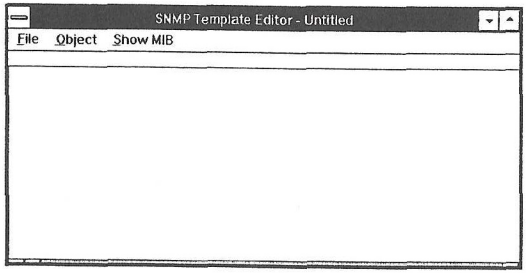
SNMP Template Editor

With the SNMP Template Editor, you can edit the pre-defined templates or create your own templates that contain selected MIB variables. You can build your own library of MIB variable collections to be used on SNMP devices throughout the network. Before creating new templates, it is important to know what MIBs you want to group together.

To access the SNMP Template Editor, complete the following procedures:

1. Choose Template Editor from the Options menu.
   The SNMP Template Editor window appears. See Figure 5-2.

Figure 5-2 SNMP Template Editor Window

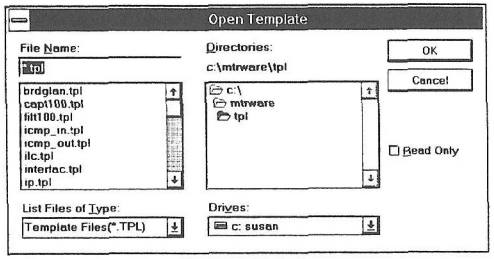


Open an Existing Template

All template files have a .tpl extension. To open an existing template, complete the following procedures:

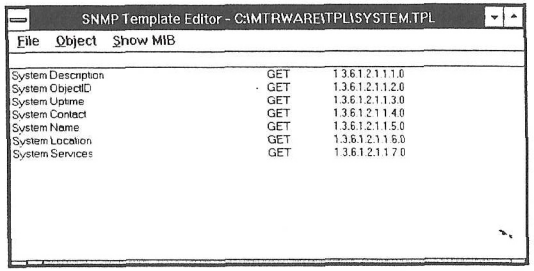
1. Choose Open from the File menu.
   The Open Template window appears. See Figure 5-3.

Figure 5-3 Open Template Window



2. Select the desired template file.
3. Click OK.
   The selected template appears in the SNMP Template Editor. See Figure 5-4.

Figure 5-4 SNMP Template Editor Window With Data



The first column in the SNMP Template Editor is the label (or name) of each MIB variable or MIB table.

The second column shows either GET or TABLE. GET indicates it is a MIB variable. TABLE indicates it is a MIB table.

The last column is the object ID string for the MIB variable. MIB tables do not have object ID strings.

NOTE: You can display the Edit GET MIB window or the Edit Table Entry window by double-clicking the related entry on the SNMP Template Editor window.

Create a New Template

Up to 30 MIB variables can be added to each template. MeterWare can display up to five templates at one time. This section assumes the SNMP Template Editor window is displayed.

To create a template, complete the following instructions:

1. Choose New from the File menu.

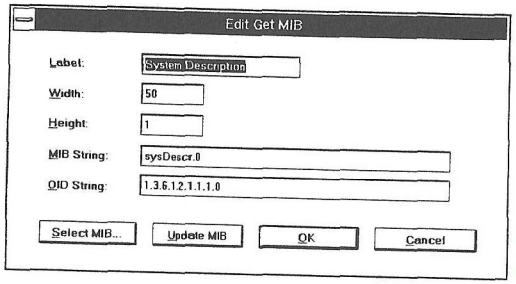
   All previous data is cleared from the SNMP Template Editor window.

2. Choose Edit Get MIB from the Object menu.

   The Edit GET MIB window appears. See Figure 5-5.

   Edit Get MIB allows for the definition of a single object instance.

Figure 5-5 Edit GET MIB Window

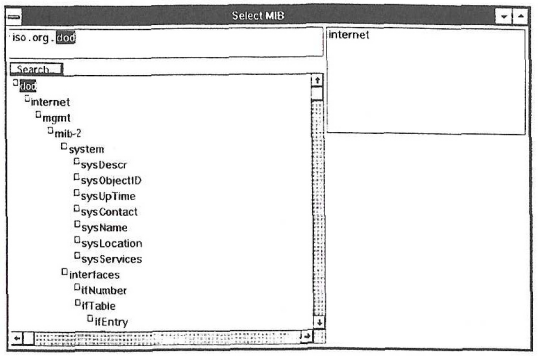


The window may already have information on it, depending upon the active MIB variable. The fields can be changed by typing over them.

3. Click Select MIB.

   The Select MIB window appears. See Figure 5-6.

Figure 5-6 Select MIB Window



The Select MIB window contains a listing of SNMP MIB variables in a tree format.

4. Traverse the tree and click the MIB variable you want to add to the template.

NOTE: You can jump to the MIB variable by clicking Search and entering the variable name in the Find field. However, the search must begin at the top of the tree. If the MIB variable you are looking for is above the current location, the system cannot find the variable.

5. Click Update MIB on the Edit GET MIB window.

   The variable's MIB string and OID string (Object Identifier string) appear in the respective boxes. The OID string represents the specific instance of the variable.

6. Double-check the OID string. Depending upon whether or not the object is a single instance, the string may need to be modified.
7. Type a <name> for the variable in the Label field.
8. Type the <width> in the Width field. Width refers to the character width of the label. The maximum character width is 50.

9. Enter <1> for Height. (Currently, the SNMP templates feature only supports a Height field value of 1).
10. Click OK.

    The MIB variable appears in the SNMP Template Editor window.

Once you have added all of the new MIB variables to the template, make sure you save them.

Delete a MIB Variable

To delete a variable from the template, click the variable you want to delete and choose Delete from the Object menu.

Add Tables to a Template

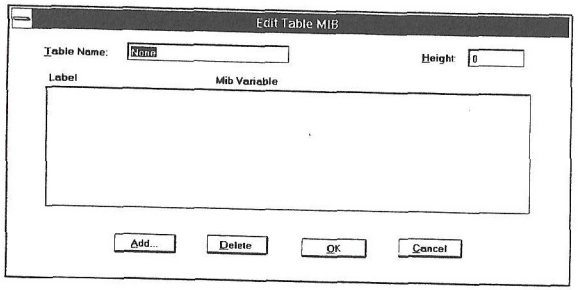
You can define a table and the number of columns and rows for the table. Each column defines a MIB variable the SNMP DA feature will perform a GET-NEXT request on. MeterWare supports up to 10 columns per table and up to five tables per template.

To add tables to the template, complete the following procedures:

1. Choose Edit Table MIB from the Object menu.

   The Edit Table MIB window appears. See Figure 5-7.

Figure 5-7 Edit Table MIB Window



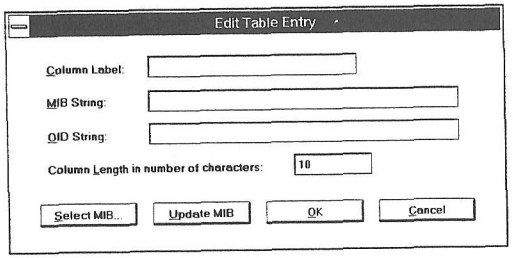
2. Type a <name> in the Table Name box.
3. Type the <table height> in the Height box.

   The table height is the number of rows displayed on the SNMP DA window for this table. The SNMP template GETs all MIB instances and you can scroll the window up or down to view the data

4. Click Add to add a MIB variable entry to the table.

   The Edit Table Entry window appears. See Figure 5-8.

Figure 5-8 Edit Table Entry Window



5. Click Select MIB.

   The Select MIB window appears. The Select MIB window contains a listing of SNMP MIB variables in a tree format.

6. Traverse the tree and click the MIB variable you want to add to the table.
7. Click Update MIB.

   The variable's MIB string and OID string appear in their respective boxes.

8. Check the OID string. Depending on whether or not the object in the table is a single instance, the string may need to be modified.
9. Enter a <name> for variable in the Column Label field.
10. Enter the <number> of characters allowed in the Column Length field.
11. Click OK. The MIB variable is added to the table.

    When you are finished adding variables to the table, click OK. The new table appears in the SNMP Template Editor.

Once you have added all of the tables to the template, make sure you save the template.

Save a Template

To save a template, choose Save from the File menu. To save the existing file under a new name or to save a new file, choose Save As from the File menu.

Template files must be stored in the MTWARE\TPL directory. In addition, each file must have a .TPL file extension; for example, Test.TPL.

Template Editor Example

In this example, we create a new template containing the sysUpTime and sysContact MIB variables from the System group and a host access table containing N.A.T. Enterprise MIB variables.

1. Choose Template Editor from the Options menu. The SNMP Template Editor window appears.
2. Choose Edit Get MIB from the Object menu.

   The Edit GET MIB window appears.
3. With the mouse, click the title bar of the Edit GET MIB window and pull it down to the lower portion of your screen.
4. Click Select MIB.

   The Select MIB window appears. The Select MIB window contains a listing of SNMP MIB variables in a tree format.
5. Traverse the tree and click on the sysUpTime variable.
6. Click Update MIB.

   The variable's MIB string and OID string appear in their respective boxes. The OID string represents the specific instance of the object.

   NOTE: Depending upon whether or not the variable (sysUpTime) is a specific instance, you may need to modify the OID string. According to its MIB definition, the specific instance of the MIB variable sysUpTime is sysUpTime.0. You must append ".0" (zero) to its OID string.
7. Type <System Uptime> in the Label field, overwriting the existing data.
8. Type <25> for the character Width.
9. Enter <1> for the Height. (At this time, MeterWare only supports a Height field value of 1.)
10. Type <.0> (period zero) on the end of the OID String.

11. Click OK.

    The newly-defined MIB variable appears in the Template Editor window. (Each MIB variable represents a GET operation that the application performs.)
12. Repeat steps 2–4.
13. Select sysContact from the MIB tree.
14. Click Update MIB.

    The variable's MIB string and OID string appear in their respective boxes.

    Again, the specific instance of the MIB variable sysContact is sysContact.0, so you must append .0 to its OID string.
15. Type <System Contact> in the Label field, overwriting the existing data.
16. Type <25> for the character Width.
17. Enter <1> for the Height.
18. Type <.0> on the end of the OID string.
19. Click OK. The two newly-defined MIB variables appears in the template editor window.
20. Select Edit Table MIB from the Object menu to add a configuration access host table to this template. The Edit TABLE MIB window appears.
21. Enter <Access> as the Table Name.
22. Enter <6> as the Height. This specifies the Access table to have six display rows.
23. Click Add to display the Edit Table Entry window .
24. Click Select MIB. The Select MIB window appears.
25. Traverse the tree and click on the cfAcchostHostIP variable.
26. Click Update MIB. The variable's MIB string and OID string appears in their respective boxes.

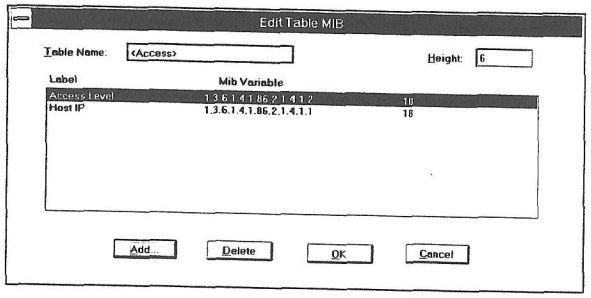
    Since the MIB variable cfAcchostHostIP has multiple instances, its OID string does not need to be modified. (For more information on the cfAcchostHostIP variable, refer to the N.A.T. SNMP User's Guide.)
27. Type <Host IP> in the Column Label field for the variable's name.
28. Type <18> in the Column Length field for the column character length.
29. Click OK. The newly-defined MIB variable appears in the Access table.

30. Repeat the process for the following MIB variable:

    cfAcchostLevelLabel = Access Level

    Once these MIB variables are added, the Access table should look like following figure. See Figure 5-9.

Figure 5-9 Edit Table MIB Window



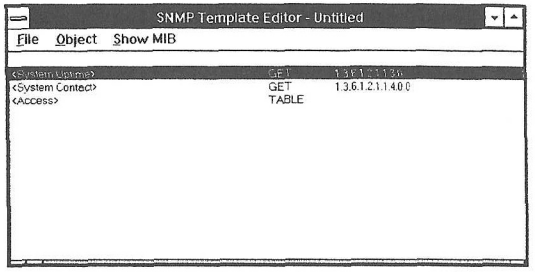
Each column in the table represents a MIB variable in an SNMP table. In this example, we are creating the N.A.T. Enterprise-specific Access Host Table. There are two MIB variables in the N.A.T.-Enterprise-specific Access Host Table, so this table will have two columns.

The SNMP template feature takes all of the column MIB variables and performs a GET-NEXT operation on them in one GET-NEXT request. Thus, it is important that all columns have the same number of instances.

31. Click OK.

    The Access table appears in the template editor window. See Figure 5-10.

Figure 5-10 SNMP Template Editor Window



32. Select Save As from the File menu to save the newly created template.

    The Save Template As window appears.

33. Type <Access.tpl> in the File Name field.
34. Click Save.
35. Exit the SNMP Template Editor by choosing Exit from the File menu.

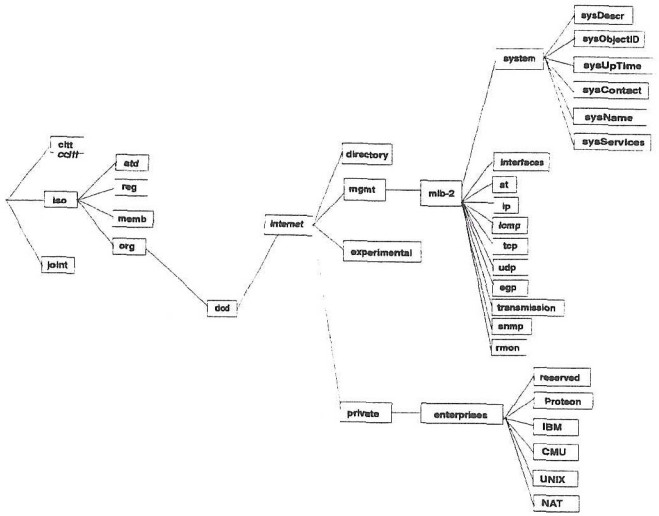
SNMP Utility

MeterWare includes SNMP Utility for use with SNMP managed devices, including other vendor's SNMP devices. The tool is used to interactively view and change management information on SNMP managed devices on the network.

MIB variables are used for monitoring and managing the network. In addition to the standard MIB-1 and MIB-2 variables found in SNMP devices, SNMP Utility includes RMON MIBs, experimental MIBs and N.A.T.'s private MIBs.

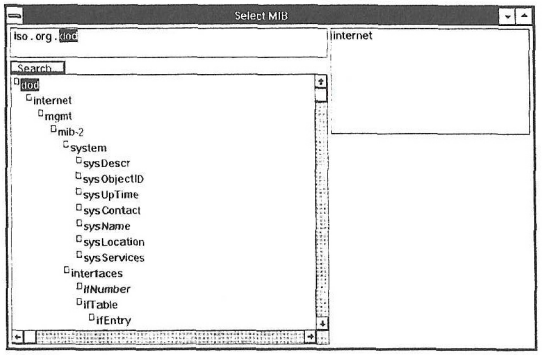
Other vendor's MIBs can be installed for use with the SNMP Utility. The following figure graphically illustrates a generic MIB variable diagram. See Figure 5-11.

Figure 5-11 Generic MIB Diagram



The MIB variables are structured as a tree. See Figure 5-12.

Figure 5-12 MIB Tree



The tree contains a root connected to labeled nodes. The labeled nodes can be subtrees with children of their own. The leaves of the tree are objects and each object has its own identifier that describes the path through the tree. The leaf attributes include:

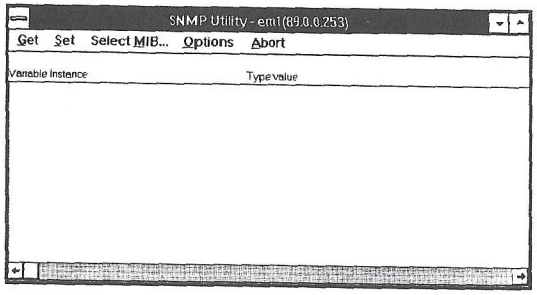
- Label
- OID (Object Identifier)
- Object Type
- Access
- Status

MeterWare is limited to viewing the MIB variables prescribed by its access level. An access level determines what portion of the tree the host can access. A MeterWare host with Read_Write access can access all MIB information and issue SET commands. A MeterWAre host with Read_Trap access can view all the MIB variables, including trap messages. A MeterWare host with Read_Private access can view all the public and private MIB variables. A MeterWare host with Read_Public information can only view MIB-1 and MIB-2 information.

To access SNMP Utility, complete the following procedures:

1. Click a device on the Network Map (for example, an EtherMeter).
2. Choose SNMP Utility from the Tools menu.
   The SNMP Utility window appears. See Figure 5-13.

Figure 5-13 SNMP Utility Window

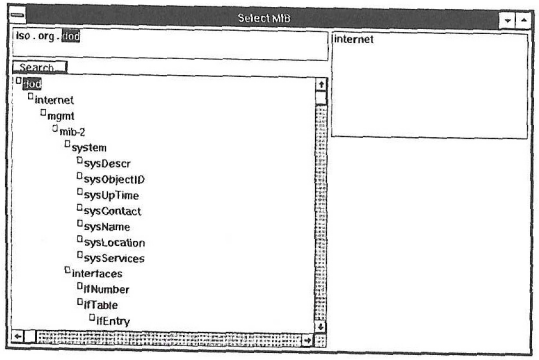


GET, SET and Search

The Select MIB option displays the MIB tree. From the Select MIB window, you can perform GET and SET operations. A Search button assists you in locating MIB objects.

To access the MIB tree, click on the Select MIB option on the menu bar of the SNMP Utility window. The Select MIB window appears. See Figure 5-14.

Figure 5-14 The Select MIB Window



The Select MIB window contains several "boxes." The long box at the top of the window (above the Search button) shows the current path of the MIB tree. The box on the right side contains a listing of the sub-trees of the current node. The large box below the Search button shows the selected portion of MIB tree.

The colors on the SNMP Utility window indicate the following:

Magenta	The current selection.
Blue	The children (leaves) in the tree.

In the example above, dod (highlighted in the upper box) is the root path. The dod structure is shown in the box below the dod box. In the graphical tree, system (highlighted) is the labeled node and its children (sysDescr, sysObjectID, etc.) are listed in the box to the right.

MIB variables in each window can be selected by double-clicking. When you double-click on a labeled node, it becomes the current node on the tree, its sub-trees appear and all boxes within the Select MIB window are updated.

When you double-click on a leaf in the graphical tree, it becomes the current node on the tree. In addition, when a leaf is selected in the tree, its attributes appears to the right of the tree.

The GET option retrieves the selected MIB information from the device. A group of objects can be obtained by selecting a non-leaf node in the tree and clicking on GET.

SET Operations

Sets the desired values of MIB variables to the device. Only a leaf should be selected for a SET operation. For MeterWare devices, only a host with Read_Write permission can use SET successfully.

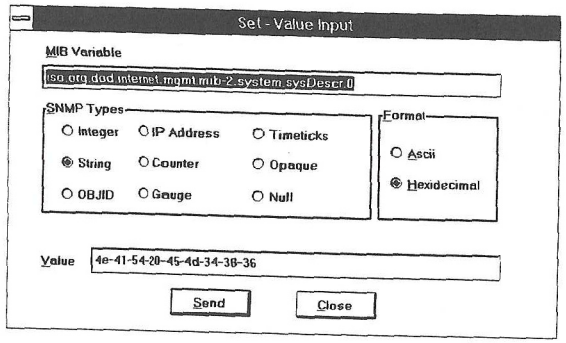
To SET a MIB variable, complete the following procedures:

1. Choose Select MIB from the SNMP Utility menu bar.
2. Choose the desired leaf (MIB variable) from the tree by clicking once on it.
3. Click Get to retrieve all of the instances of the MIB variable.

   If a GET operation cannot be performed on the MIB variable, simply select the variable from the MIB tree and click Set. The Set–Value Input window appears, as described in the next step.
4. Choose an instance from the list by double-clicking on it.

   The Set–Value Input window appears. See Figure 5-15.

Figure 5-15 Set–Value Input Window



The Set–Value Input window shows the MIB variable instance and data type.

5. Specify the type by clicking on the appropriate radio button in the SNMP Type box.
6. Specify the format for the value by clicking on the appropriate radio button in the Format box.
7. Enter the desired <value> in the Value dialog box. (A listing of the MIB object attributes, including access modes and values, that MeterWare's SNMP managed devices support can be found in the N.A.T. SNMP User's Guide.)
8. Click Send to send the data to the device.
9. Click Close when you are finished.

   If an unsuccessful SET command occurs, MeterWare reports "Message error: Operation NOT Successful." Verify that your MeterWare station has the appropriate access level.

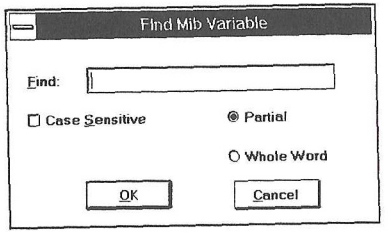
Search the MIB Tree

The Search option traverses the MIB tree, seeking a specific variable.

To search for a MIB variable, complete the following procedures:

1. Click Search to display the Find MIB Variable window. See Figure 5-16.

Figure 5-16 Find MIB Variable Window



2. Enter the <MIB variable string> (or partial string) in the Find field.
3. Select the additional parameters as desired.
4. Click OK. The search starts from the current selected node of the graphical tree. When the object is located, it is highlighted.

SNMP Utility Examples

The way MIB objects are used to manage the network is fundamentally the same for all types of network management tools. The user interface may vary among the different types of SNMP software tools, but the underlying MIB management procedures are the same.

Some examples of how to use MIB objects with MeterWare's SNMP Utility are given below.

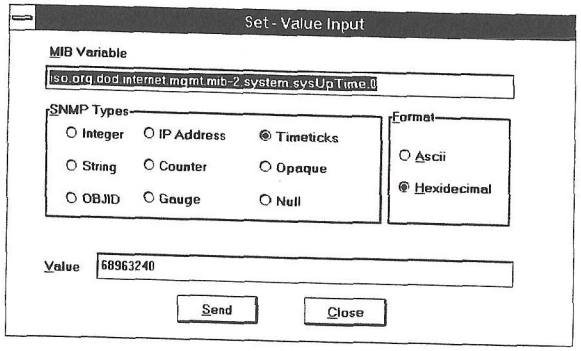
Example 1: GET and GET-NEXT

This example shows how to perform GET-NEXT and GET operations to retrieve System Group MIB information from a particular device on the network.

1. Click a device on the Network Map (for example, an EtherMeter).
2. Choose SNMP Utility from the Tools menu.
3. Click Select MIB to view the Select MIB window.

4. Click System in the subtree.
5. Click Get to perform a GET-NEXT operation on the System Group. This displays all instances of the System Group supported by the particular device selected.
6. Double-click one of the variable instances within the System Group to perform a GET operation. In this example, a GET operation is performed on the instance sysUpTime. The Set–Value Input window appears. See Figure 5-17.

Figure 5-17 Set–Value Input Window



The value of sysUpTime appears in the Value box (60963240) and the object's SNMP Type is shown (timeticks). Click Close when you are finished viewing this window.

Example 2: Activate and Deactivate Tables

This example shows how to deactivate and reactivate the tables in the RMON Host group using SNMP SET commands.

1. Click a device on the Network Map (for example, an EtherMeter).
2. Choose SNMP Utility from the Tools menu.

   The SNMP Utility window appears.
3. Click Select MIB... to view the full Select MIB window.
4. Double-click internet in the tree to find the RMON group under the management sub tree.

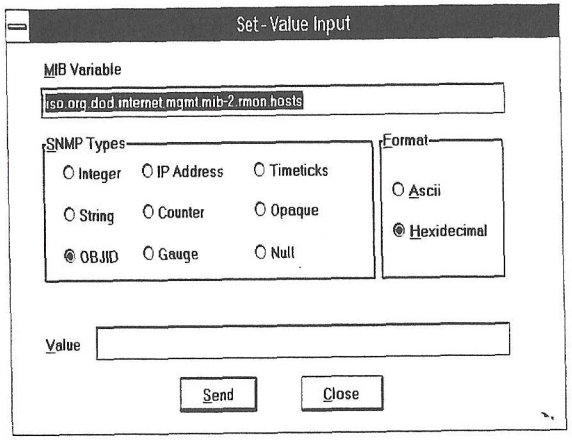
   The internet sub-trees display in a box in the upper-right corner of the window.

5. Double-click mgmt in the upper-right corner box
6. Double-click mib-2, rmon, hosts, hostControlTable, hostControlEntry and hostControlStatus respectively.

NOTE: For some versions of MeterWare, RMON is under the experimental subtree. If this is the case, the path you would take is internet, experimental, rmon, etc.

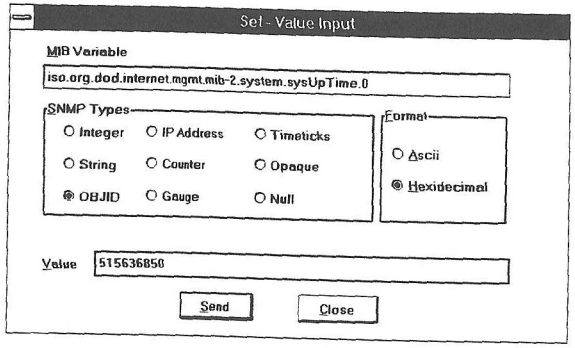
The entire tree path displays in the long box at the top of the window. When you double-click on any item in the long box, the MIB tree is updated. For example, if you double-click on hosts, the MIB tree updates the host sub-tree. See Figure 5-18.

Figure 5-18 Select MIB Window



7. Click Set. The Set–Value Input window appears.
8. Enter the <object identifier> for the hostControlStatus MIB variable. (Refer to the MeterWare SNMP User's Guide, for the object identifier.)
9. Change the hostControlStatus.0 to hostControlStatus.1 by entering <4> (for invalid) in the Value box. See Figure 5-19.

Figure 5-19 Set–Value Input Window



10. Click Send to send the information to the device. Assuming your host has the read-write access level, the operation should be successful. The hostControlTable, hostTable and hostTimeTable are deactivated.
11. Do a GET operation on hosts under the rmon group to verify that the three tables under the hosts group have been deactivated. Nothing appears in the tables.

Reactivate Tables

To reactivate the tables, create the tables and then activate them. To do this, complete the following procedures:

1. Click internet in the tree to verify that the three tables under the host group have been de-activated. The internet sub-trees display in a box in the upper-right corner of the window.
2. Double-click mgmt in the box.

   Double-click mib-2, rmon, hosts, hostControlTable, hostControlEntry and hostControlStatus respectively.
3. Click Set.

   The Set – Value Input window appears.
4. Enter the <object identifier> for the hostControlStatus MIB object. Change the hostControlStatus.0 portion to hostControlStatus.1 and enter <2> in the Value box. (A value of 2 indicates that you want to create the tables.)
5. Click on Send to send the information to the device. Assuming your host has the read-write access level, the operation should be successful. The hostControlTable is created. However, the hostTable and hostTimeTable still need to be activated.
6. Select the hostControlStatus object again.
7. Change the hostControlStatus.0 portion to hostControlStatus.1 and enter <1> in the Value box. (A value of 1 indicates that you want to validate the tables.)
8. Click on Send to send the information to the device. Assuming your host has the read-write access level, the operation should be successful. The hostControlTable, hostTable and hostTimeTable is activated.

Verify the Active Tables

Verify that the three tables under the hosts group have been activated. Do a GET operation on hosts under the rmon group. The tables appear in the tree.

MIB Compiler

You can compile MIB text files supplied by N.A.T. or other vendors, without leaving MeterWare. Once a MIB text file is compiled it can be loaded into MeterWare. The MIBs become part of the MIB tree and can be accessed through the SNMP Utility.

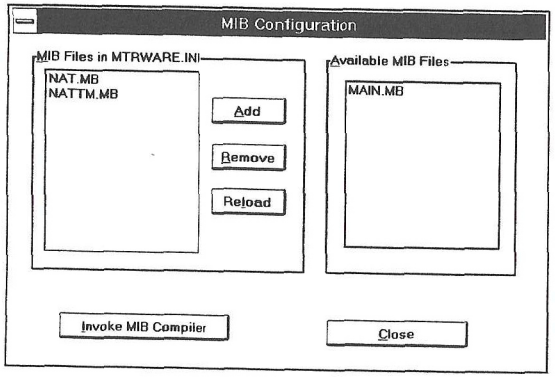
NOTE: Although N.A.T. supplies MIB text files from other vendors, N.A.T. recommends you obtain the latest file directly from the vendor.

To compile a MIB text file, complete the following procedures:

1. Choose MIB Configuration from the Options menu.

   The MIB Configuration window displays. See Figure 5-20.

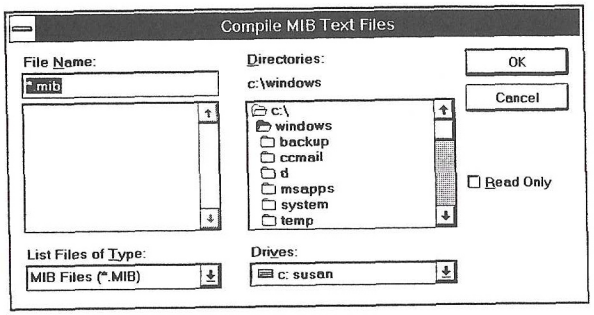
Figure 5-20 MIB Configuration Window



2. Click the Invoke MIB Compiler button.

   The Compile MIB Text Files window appears. See Figure 5-21.

Figure 5-21 Compile MIB Text Files Window



3. Click the desired MIB file.
4. Click OK.

   You are notified that the compiler is running. When the message clears, the MIB Compiler Messages window displays.

   The MIB Compiler Messages window displays messages, warnings and errors generated during the compile process. If you want to save the information into a disk file, click the Save As button to display the Save As screen. Type the name of the file in the File Name field and click OK. The apparent error was generated intentionally.

5. Click Close to exit the window.

   The Vendor MIB Files Configuration window displays.

6. Click Close to return to the map.

MIB Compiler Run

As mentioned previously, when the system completes the task of compiling a MIB text file into a binary file, it displays the MIB Compiler Messages window.

The first line in the window describes the MIB compiler and the file it compiled. The error message (line 61) was generated intentionally to show a compiler error. The "Writing" statement describes the level where the file is rooted and the name of the binary MIB file. Binary MIB files have .MB extensions. (MIB text files have .MIB extensions.) The last line is a "Done" statement, indicating the target binary MIB file was created.

Unless the compiler is unable to write the binary file due to some physical limitation, the MIB text file is unconditionally compiled into a binary file. Limitations include attempting to overwrite a read only file or a lack of physical space on a drive. In other words, unless there is a physical restriction on the target binary file, the binary file is created, errors and all. The MIB Compiler does not stop or abort the process because an error is encountered.

MIB File Format

You may want to create a MIB file from a MIB group or split a file that is too large for the compiler. This section describes some compiler basics that will help you assemble a MIB text file.

The MIB Compiler is limited to 8,000 leaf nodes and 256 characters per line (including comments). If the MIB you intend to use exceeds these limits, edit the file to eliminate the MIB groups that are either duplicated elsewhere (such as MIB-2) or MIB groups you will not be using for that SNMP agent and reduce the length of the character strings.

The number of nodes may be further limited by the memory or disk space available on an individual computer. N.A.T. recommends a maximum of four MIB files loaded at one time. The system accepts more than four, but performance suffers.

MIB Text Format

Before you can correct errors, it is helpful to understand the structure of MIB text. The format follows industry standards. N.A.T.-specific MIBs include ASN.1 codes for each MIB object. The following figure shows a MIB Object. See Figure 5-22.

Figure 5-22 A MIB Object

```
downloadServerIP OBJECT-TYPE
-- ASN.1 CODES          NAT.2.3.4.1.0
        SYNTAX          IpAddress
        ACCESS          read-write
        STATUS          mandatory
        DESCRIPTION
        "IP address of the TFTP server where
        the FLASH code will be downloaded."
        ::= { downLoadControl 1 }
```

OBJECT-TYPE is the name of the MIB. OBJECT TYPE is also know as OBJECT DESCRIPTOR.

ASN.1 CODES are the explicit object identification used in SNMP operations to identify the tree path. A double dash ( ) in front of the code indicates a comment. The standard RFC format does not include ASN.1 code descriptions.

SYNTAX is the data type that models the MIB object.

ACCESS is the community string (authentication and authorization) access level. The access level may be read-only, write-only, read-write or not-accessible.

STATUS is the general status of the MIB. The possible levels are:

- Mandatory: Managed nodes must implement this object. If this group is implemented, this MIB variable must be included.
- Optional: Managed nodes may implement this object.
- Obsolete: Managed nodes do not need to implement this object.

DESCRIPTION is a textual definition of the MIB object.

::= symbol shows the parent and the number of levels the MIB is from that parent.

Warning Messages

Warning messages are advisory; they do not require correction for the MIBs to compile correctly. Warning messages are displayed in the MIB Compiler Messages window. The message includes the line number where the error was trapped. A list of warning messages follow.

Warning: found a zero-valued integer sub-id	Values in integer sub-id fields should not be zero. The system accepts a zero value, but warns you of the condition.
Warning: found a zero-valued enumeration integer	Values in enumerated integer fields should not be zero. The system accepts a zero value, but warns you of the condition.
Warning: missing integer sub-id	The compiler expected to find a sub-id, but did not. The sub-id is not required, but the compiler warns you of the condition.
Warning: truncated MIB variable name xxxx	The name of the MIB variable (OBJECT-TYPE) exceeded the length limit standard (250 characters) and was truncated from the right by the compiler.

Error Messages

Errors may cause the MIB to function unpredictably or not at all. Most errors are caused by typographical errors in the source MIB text file. The errors can be corrected by opening the file with a text editor and correcting the error. When errors are trapped by the compiler, the results are displayed in the MIB Compiler Messages window. (Some error messages display the questionable data found by the compiler. In the error messages below, xxxx represents the data found by the compiler.)

ad object id sequence	The length of the object identifier is less than zero.
Expecting an integer sub-id, but found xxxx	An integer was expected, but the compiler found an undefined character string.
Expecting (, but found a space character	The compiler expected an open parenthesis, but found a space instead.
Expecting), but found a space character	The compiler expected a close parenthesis, but found a space instead.
Expecting), but found EOF	The compiler expected a close parenthesis, but found an end-of-file mark instead.
Expecting {, but found EOF	The compiler expected an open bracket, but found an end-of-file mark instead.
Expecting }, but found EOF	The compiler expected a close bracket, but found an end-of-file mark.
Expecting {, but found xxxx	The compiler expected an open bracket, but found an undefined character string.
Expecting { or OF, but found xxxx	The compiler expected an open bracket or OF, but found an undefined character string.
Expecting semicolon, but found EOF	The compiler expected a semicolon, but found an end-of-file mark instead.
Expecting ::=, but found EOF	The compiler expected a ::= symbol, but found an end-of-file mark instead.
Expecting ::=, but found xxxx	The compiler expected a::= symbol, but found an unknown character string.
Expecting an object id, but found EOF	The compiler expected an object identifier, but found an end-of-file mark instead.
Expecting an object id, but found xxxx	The compiler expected an object identifier, but found an unknown text string.

Expecting a label, but found xxxx	The compiler expected a label, but found an unknown text string.
Expecting SYNTAX, but found xxxx	The compiler expected the identifier SYNTAX, but found an unknown text string.
Expecting a syntax type, but found xxxx	The compiler expected a syntax type, but found an unknown text string.
Expecting ACCESS, but found xxxx	The compiler expected the label ACCESS, but found an unknown text string.
Expecting an access type, but found xxxx	The compiler expected an access type, but found an unknown text string.
Expecting STATUS, but found xxxx	The compiler expected the label STATUS, but found an unknown text string.
Expecting a status, but found xxxx	The compiler expected a status entry, but found an unknown text string.
Expecting a label, but found a keyword: xxxx	The compiler expected a label, but found an unknown text string.
Expecting BEGIN, but found xxxx	The compiler expected the label BEGIN, but found an unknown text string.
Expecting a keyword, but found xxxx	The compiler expected a keyword, but found an unknown text string.
Line buffer is full ****xxxx	The MIB variable is greater than 256 characters and is not in standard MIB format.
No ending integer sub-id	The length of the object identifier (ASN.1 Codes) is less than two or greater than 20.
Missing ending integer sub-id	The length of the object identifier (ASN.1 Codes) is less than zero.
No terminating parenthesis	The closing parenthesis is missing.
Premature end of file	An end-of-file mark was found before it was expected. The file may be corrupt.
Parents of the following nodes are missing:	The compiler was unable to identify the parents of the MIBs that follow.

Binary File Errors

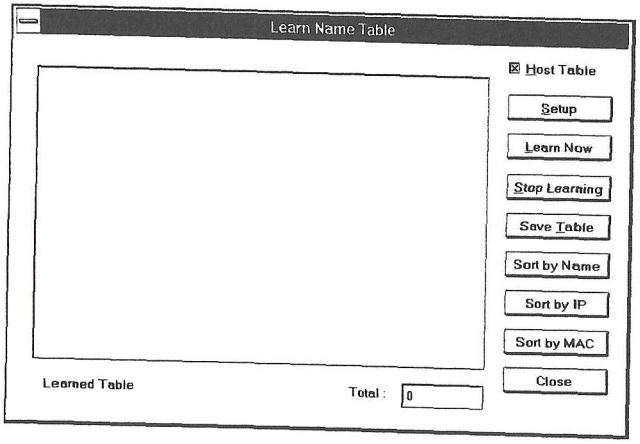
Binary file errors are usually the result of the compiler's inability to either create or write to the specified binary MIB file. These errors are usually fatal, in that the system fails to create the binary version of the .MB file.

No more space for malloc	The binary MIB file is limited to 10 segments of 64KB each, which allows for 8000 leaf nodes. If the system exceeds this limitation, the binary MIB file is not created.
Too many defined new types: MAX_NEWTYPE is 10	The maximum number of new object types is 10. If the MIB text file contains more than 10, this message displays.
Lost root of node list xxxx	The structure of the MIB text file is incorrect.
The file is not accessible	The system was unable to find the target file.
MIB file is bad	The MIB text file is not a text file or the file is not in the proper format.
No root existing for this MIB file xxxx	The structure of the MIB text file is incorrect.
No root is found xxxx	The structure of the MIB text file is incorrect.

Learn

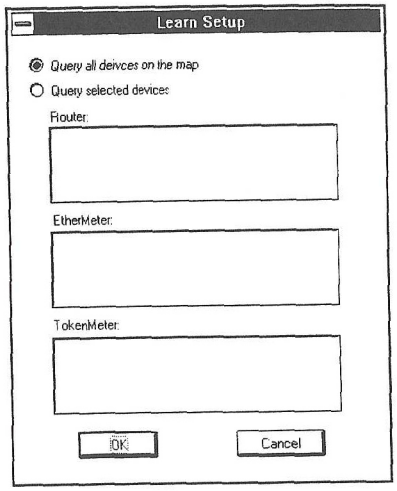
The Learn Window allows you to search for device information either from local data on the MeterWare host or from different services available on the various network devices. When the host table check box is selected MeterWare will start searching for device information from different devices and services on the network.

Figure 5-23 Name Editor Learn Window



The learn process can take a variable amount of time depending on the size and configuration of the network. Select the Setup button to access the Learn Setup dialog window. You can customize the learn search by selecting specific devices or you can search all devices on the network map.

Figure 5-24 Learn Setup Dialog



When the Host Table check box is selected MeterWare searches in this order the following files and services:

- Host Table
- DNS (if it is enabled)
- Win Services
- LanManager Hosts

The default parameters for the search are 2 retries with a 2 second timeout. With large networks the search could take a substantial amount of time.

Name Editor

The Name Editor manages Name tables containing numeric values and corresponding text strings that are substituted in many MeterWare windows. There are four Name tables. These tables are listed and described below:

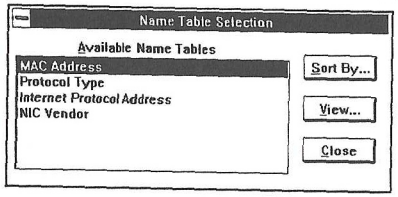
MAC Address	Contains device names associated with Ethernet and Token Ring MAC addresses
Protocol Type	Contains text strings matching the network layer protocol types
Internet Protocol Address	Contains device names associated with IP addresses
MAC Vendor	Contains vendor names associated with vendor ID field of the MAC address

The Name tables provided by N.A.T. can be customized. You can add, edit or delete names from the tables. The editing can be done on-line throughout MeterWare or off line using an ASCII text editor. Each Name table can include up to 2000 entries.

To access the Name Editor, complete the following procedures:

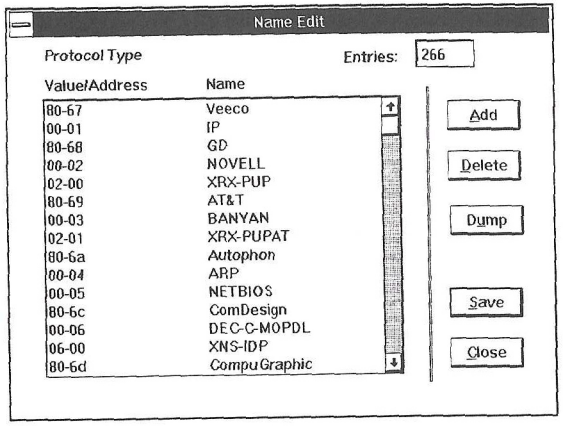
1. Choose Name Editor from the Options menu to display the Name Table Selection window. See Figure 5-25.

Figure 5-25 Name Table Selection Window



2. Click any table in the Name Table Selection window.
3. Click the View button to view information about a Name table. The table displays in the sort order specified. See Figure 5-26.

Figure 5-26 Name Edit Window



Names that have been defined from a device's information tab are automatically put into the Name Editor. Those entries have an asterisk at the end of the entry. Marked entries may not be deleted or modified through the Name Editor. They can only be changed through the Edit Device feature.

Sort a Name Table

The Name tables can be sorted by name or by value. To choose the sort criteria for the tables, complete the following procedures:

1. Click Sort by to display the Sort Selection window.
2. Click the desired sort criteria.
3. Click OK.

Edit a Name Table Online

Names can be added or deleted from the Name tables through MeterWare.

Add a Name to the Table

Adding a name to the chosen Name table is a simple matter. The following procedure assumes the table is already displayed.

1. Click Add to display the Value/Name Entry window.
2. Type the <address> in the Value/Address field.
3. Type the <vendor's name> in the Name field.
4. Click OK to close the window.

   You are returned to the Name Edit window.

Delete a Name from the Table

Deleting a name from the chosen Name table removes the name from the list. The following procedure assumes the table is already displayed.

1. Click the entry to be deleted.
2. Click Add to display the Value/Name Entry window.
3. Click Delete.

   The entry is removed and you are returned to the Name Edit window.

Edit a Name Table Off-line

The Name tables can be dumped into ASCII files and edited using a word processor. The Name Editor Dump feature provides an alternative to the tedious work of updating Name tables on-line. When major changes are required, the list can be dumped into an ASCII file and all the tools available in a word-processing environment can be used for off-line editing.

Once an ASCII Name file is edited, it is compiled back into its binary form off-line, using the Name Compiler utility, MTR_NAME.EXE, found on the Utility disk. The files corresponding to the Name tables are as follows:

NAME TABLE	BINARY FILE	ASCII FILE
MAC Address	ETHER.NBM	ETHER.NAM
Protocol Type	ETHERTP.NBM	ETHERTP.NAM
Internet Protocol Address	IP.NBM	IP.NAM
MAC Vendor	VENDOR.NBM	VENDOR.NAM

For example, you could dump the Internet Protocol Address table to the ASCII file IP.NAM. Edit the file with a word processor and use the MTR_NAME utility to compile it back into the IP.NBM file. (IP.NBM is the binary version of the file MeterWare reads when it loads.)

The basic process for the off-line modification of a Name table is as follows:

1. Dump the files you want to modify. When you do a dump, the files are automatically exported the default MeterWare subdirectory you specified when MeterWare was installed.
2. Edit the file. The file is in ASCII and any editor used should have the capability of saving the file back to ASCII. Comments are allowed in the ASCII file. The pound sign (#) on the first character of a row indicates a comment line.
3. Compile the file. The compiler can be launched from a DOS prompt or a Run request in either the Windows File Manager or the Program Manager.

ASCII File Layout

The ASCII file is divided into two columns. The first column contains the value in related formats (e.g., decimal, hexadecimal or mixtures). The second column contains the symbolic name. An example of a Name table is presented below:

```
0000a3-b8019c     NAb8019c     *
0000a3-8034a4     bridge1      *
0000a3-b006a6     NAb006a6     *
ffffff-ffffff     broadcast
0000a3-8034ba     NA8034ba     *
0000a3-a005e7     NAa005e7     *
123456-7890ab     UN7890ab     *
0000a3-a00808     ILCConc      *
0000a3-a80020     NAa80020     *
0000a3-e00008     NAe00008     *
0000a3-901c3d     NA901c3d     *
0000a3-a80141     NAa80141     *
0000a3-b00346     NAb00346     *
```

The asterisk (*) is found in the MAC Address and the Internet Protocol Address files. It is appended to the end of the entry to indicate the address was found in the MeterWare database and cannot be changed. The system compares the Name file to the MeterWare database. If the Name file information conflicts with the MeterWare database, the system automatically overwrites the Name file with the information from the MeterWare database.

Value Column Format

For the value column, the value is specified as a byte stream value, such as decimal 32.1.2. The delimiters can be period, dash, space or nothing for hex format. The format can be:

Decimal: A delimiter is necessary and can be any non-alphanumeric character, such as 18.34.20 or 12-192-56.

Hexadecimal: A delimiter is necessary and can be any hexadecimal character, for example: 0000A3A00035 or 080032452378.

Mixture: Mixture of decimal and/or hexadecimal. Hexadecimal must have a prefix of "0x." A delimiter is necessary and can be any hexadecimal character, for example, 89.1.23.0xfe or 0x59.12.34.67.

Symbolic Name Format

For the symbolic name format column, the name should start with a letter in the alphabet and can contain any printable characters. The line feed or optional space can serve as a name delimiter. Currently, the utility supports names with up to 12 characters.

Name Table Dump

To dump a vendor name file into an ASCII file, complete the following procedures:

1. Choose Name Editor from the Options menu.
   The Name Edit window displays.
2. Click the desired name table.
3. Click View.
   The Name Edit window displays.

4. Click Dump.
   The file is dumped to its respective ASCII file. Below is sample data from the Ethernet type Name file:

```
# XEROX
PUP
02-00          XRX-PUP
02-01          XRX-PUPUT
06-00          XNS-IDP
#Tcp/Ip
08-00          DOD-TCPIP
08-01          X.75-IP
08-02          NBS-IP
08-03          ECMA-IP
```

5. Edit the file using an ASCII text editor.
   Once the file has been edited, the next step is to recompile the Name table into binary form. The next section describes this process.

Name Table Compiler

Once the ASCII file is edited, the name data can be converted back into a file with the {*.NBM} extension for direct use by MeterWare using the name utility MTR_NAME.EXE.

1. Access the DOS prompt or the Windows Run window.
2. Type the <command string>.
   The syntax is:

mtr_name [-dlst] <input file>

Where:

-d	switch to dump development messages
-l<num>	value length (default is 6)
-s	space is a delimiter in a symbolic name
-t<ch>	"h" for hex, "d" for decimal, "m" for mixture (default is hexadecimal)

NOTE: The optional parameters can be specified by either a forward slash (/) or a dash ( ).

The following are example command line entries for each of the files:

mtr_name	ether	
mtr_name	-l2	ethertp
mtr_name	-l4 (space)	-tm ip
mtr_name	-l3	vendor

NOTE: For clarity, the first character in the second column for -l2, -l4, -l6 is a lower-case, alphabetic L, not a numeric one (1).

3. Press ENTER.
   The ASCII file is compiled into a binary file that can be used by MeterWare immediately.

Chapter 6 MeterWare Utilities

MeterWare provides the following useful utilities.

TO...	REFER TO...
Locate a device on the map	"Locate a Device," on page 116
Set parameters for and view logs	"System and Device Logs," on page 117
Download firmware to a device	"Device Firmware Download," on page 120
Ping a device	"Ping Device Window," on page 126
Poll a MIB device	"MIB Poller," on page 127

Locate a Device

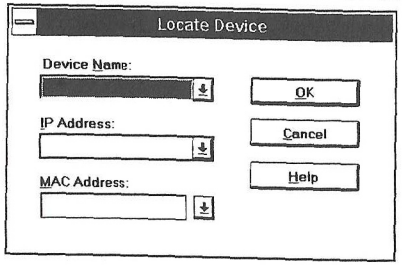
You can search for a device in the network map by name, IP address or Ethernet address. The system searches the main map and all submaps. When the system locates the device, it turns the icon magenta.

If the icon is on a submap, the system automatically displays (zooms) the submap and turns the icon magenta.

To search the map for a device, complete the following procedure:

1. Choose Locate Device from the Edit menu.
   The Locate Device by window appears.

Figure 6-1 Locate Device Window



2. Enter the <search parameter> for either the Device Name, IP Address or MAC address.
3. Click OK.
   The related parameter window clears and the icon for the chosen parameter is highlighted in magenta.
   If the system cannot find the device, you are notified that the device was not found.

System and Device Logs

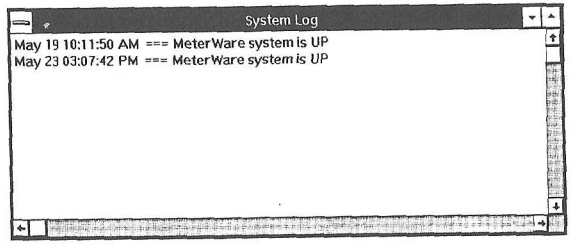
The System Log provides information about key MeterWare events and error (trap) messages. It includes a chronological listing of all the significant events that occurred within the time parameters set in the Log Parameters window. Significant events include configuring IP addresses, making the Name Server window active, setting alarms and trap messages. These messages can be viewed online or dumped to an ASCII file. The Device Log feature allows you to view messages related to a specific device.

The log window comes in two forms, the System Log and Device Log window.

To display the Meterware Log, complete the following procedures:

1. Choose System Log the Events menus.
   The System Log window appears. See Figure 6-2.

Figure 6-2 System Log Window



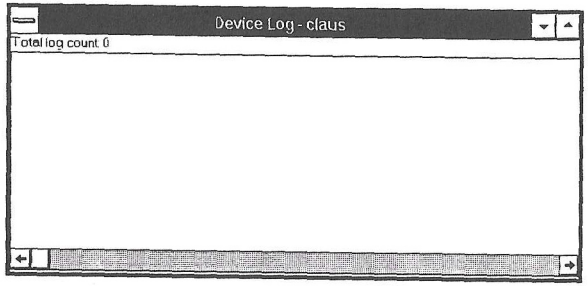
Device Log Messages

The Device Log window displays the log entries pertaining to a specific device on the network. The Device Log searches the general log for the last 512 entries associated with the selected device and displays the entries.

To display the device log, complete the following procedures:

- Choose Device Log from the Events menu. The Device Log window appears. See Figure 6-3.

Figure 6-3 Device Log Window



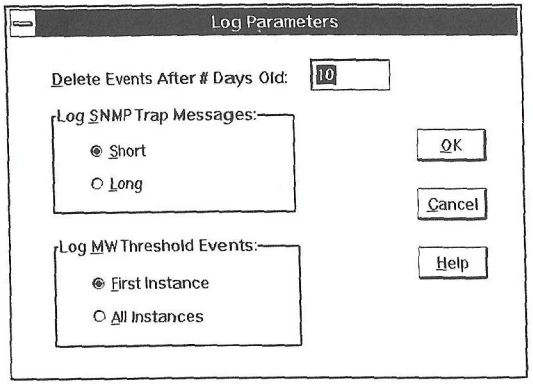
Modify Log Parameters

The Set Log Parameters window controls the length of time a message remains in the log file, the format of the messages received and threshold events.

To access the Log Parameters window, complete the following procedures:

1. Choose Set Log Parameters from the Events menu.
   The Log Parameters window appears. See Figure 6-4.

Figure 6-4 Log Parameters Window



The fields in the Log Parameters window are described below:

Delete events of # days old	You can specify the number of days events remain in the log. Events with a date stamp exceeding this limit are purged. The log is limited to 25,000 event entries. If the log reaches this limit before it reaches the limit in days, entries are deleted one day at a time until the size of the log is less than 23,000 entries.
Log SNMP Trap Messages	The amount of detail provided in each message can be set. A short message provides a date stamp, a time stamp and the message number. A long message includes a brief explanation of the message. Click the desired radio button to make your selection.
Log MW Threshold Events	You can choose how you want to log events that exceed the specified alarm threshold. Choose whether to log all instances that exceed the specified alarm threshold or just the first instance. Click the desired radio button to make your selection.

2. Modify the Log Parameters window as desired.
3. Click OK to return to the map.

Log Dump

An off-line DOS utility, LOGDUMP.EXE, dumps the contents of the log to the screen or to an ASCII data file.

To dump the binary log file into an ASCII file, complete the following procedures:

1. Display the DOS prompt.
2. Type [LOGDUMP] and the parameters to redirect it to a <user defined file>. An example of the entry is presented below:

   LOGDUMP > LOG1OUT.TXT

   NOTE: If you want to dump the log to the screen, simply type LOGDUMP at the DOS prompt.

3. Use an ASCII text editor to view the output file.

Device Firmware Download

MeterWare has a built-in TFTP server and a user interface for downloading N.A.T. Monitoring Application Software (firmware) into the EtherMeter and TokenMeter.

Select Options/Device Download from the main MeterWare menu. When MeterWare is installed, the following statement is automatically added to the MTRWARE.INI file:

```
[DOWNLOAD]
DEFAULT_DIR = c:\tftpboot
TFTP_SERV_ENABLE = TRUE
```


The entries are described in the following table:

VARIABLE	DEFAULT	DESCRIPTION
DEFAULT_DIR	c:\tftpboot	The TFTP Server searches the subdirectory specified by the DEFAULT_DIR variable, for the files containing the firmware. The subdirectory name can be modified to your own specifications.
TFTP_SERV_ENABLE	TRUE	The TFTP Server is enabled by default. To disable the TFTP Server, change the value of this variable to FALSE.

You can further automate the TFTP server to identify the firmware file and automatically download it to a specified device. The procedure for adding the proper statement to the MTRWARE.INI file is described in the next section.

Firmware Files

The firmware files are provided by N.A.T. on a disk included with the device or as part of a firmware upgrade package. The file can be selected from the file list or you can modify the MTRWARE.INI file to automatically select the file you want to download.

NOTE: The file extension matches the device. For example, the file extension for the EtherMeter/450 firmware files is 450.

An example of the MTRWARE.INI file statements is presented below:

```
[DOWNLOAD]
DEFAULT_DIR = c:\tftpboot
EtherMeter/250 = rmon240.250
EtherMeter/450 = rmon240.450
TFTP_SERV_ENABLE = TRUE
```

Add Firmware Defaults

To turn add firmware file defaults to the MTRWARE.INI file, complete the following procedures:

1. Open the MTRWARE.INI file with any text editor.
2. Locate the [DOWNLOAD] statement.
3. Type the <default file statements> on separate lines, between the DEFAULT_DIR = c:\tftpboot and the TFTP_SERV_ENABLE = TRUE statements.
4. Exit and save the MTRWARE.INI file.
5. Restart MeterWare to load the MTRWARE.INI file.

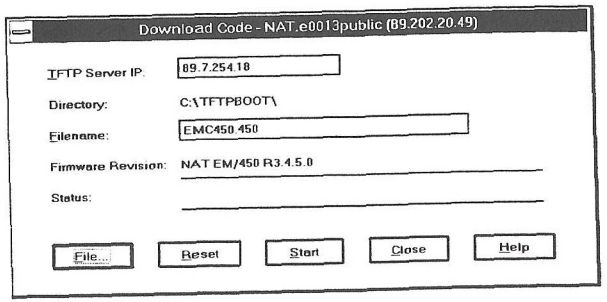
Download Firmware to a Device

Complete the following instructions to download firmware to the device:

1. Create the default subdirectory titled tftpboot.
2. Copy the firmware files from the download diskette to the default subdirectory (e.g., copy a:\rmon240.250 c:\tftpboot).
3. Bring up MeterWare.
4. Click the icon for the target device.
5. Choose Device Download from the Options menu.

   The Download Code window displays. See Figure 6-5.

Figure 6-5 The Download Code Window



The Reset button performs a hardware reset on the device.

If a device was selected for which a firmware file was specified in the MTRWARE.INI file, the Filename field displays the name of the firmware file.

If the file is not listed in the MTRWARE.INI file or you want to download a file other than the default file, you can type over the <file name> displayed.

— OR —

The File button opens a file browser window from which the file to be downloaded can be selected.

6. Click Start to download the firmware.

   A series of messages display in the Status field. If the download is successful, the following messages display, tracking the progress of the download:

   Start downloading

   Resolving hardware address

   TFTP request sent

   Downloading...

   Done

   If the operation is successful the message "Done" appears in the Status field. The version number of the firmware downloaded appears in the Firmware Revision field.

   — OR —

   If the operation was not successful, an appropriate error message displays in the Status field. You can click on Reset to restore the previous firmware version. The error messages are described in the next section.

7. Click Close to close the window.

Firmware Download Error Messages

If the download is not successful, an error message appears in the Status field. The error messages are described below.

MESSAGE	ERROR	DESCRIPTION
Invalid file format	file–verify–error (6)	Downloaded file content error. Possibly, you are attempting to download the wrong file.
Write flash memory error	flash–write–error (7)	Error occurred while writing to FLASH memory. Contact N.A.T. for assistance.
Verify flash memory error	flash–verify–error (8)	Error detected after copy to FLASH memory. Contact N.A.T. for assistance.
General timeout	time–out (9)	Either the Server IP address or the filename is not available within 60 seconds after the status is set to start–downloading (1).
Invalid file	invalid–file (10)	The file format is not correct. Possibly the file specified is not a firmware download file.

MESSAGE	ERROR	DESCRIPTION
Timeout, unreachable destination	time–out–address (11)	The hardware address was unresolved in 100 seconds. There was no response from the TFTP server within the allotted time.
Timeout, no TFTP response	time–out–request (12)	The TFTP read request was not answered in five retries. The EtherMeter retries once every five seconds. Possibly, the IP node does not support TFTP.
Timeout, download data	time–out–download (13)	File transfer not completed. Whenever the EtherMeter fails to receive the proper TFTP data packet, it retransmits the last packet every five seconds. It aborts after five retries.

The following error messages are defined as 100 plus the TFTP Error Codes returned by the server:

NUMBER	DESCRIPTION
100	Not defined. An unanticipated error occurred.
101	File not found. The system was unable to locate the file specified.
102	Access violation. The system could not access the file due to a security access violation.
104	Illegal TFTP operation. The requested operation is not allowed by the TFTP.
105	Unknown transfer ID.

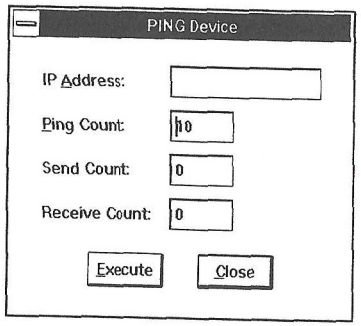
Ping Device Window

MeterWare can poll any IP device on the network to determine its up or down state.

To ping a device, complete the following procedures:

1. If the device's IP address is defined in MeterWare, select its icon from the map.
2. Choose Ping Device from the Tools menu. The Ping Device Window appears. See Figure 6-6.

Figure 6-6 Ping Device Window



3. If you selected the device, its IP Network Address appears on the Ping Device window.

   — OR —

   Enter the <IP address> of the device you want to ping in the Network Address dialog box.
4. Enter a <count> in the Ping Count field or accept the default.
5. Click Execute to begin sending packets. If the device is operational, every packet sent should be echoed by the device and counted in the Receive Count.

MIB Poller

To define a data set (i.e., add a session) and start the polling process, you use the MIB Poller tool. It is possible to have the N.A.T. Meter Reporting System installed on the same machine on which you have MeterWare for Windows installed. You should be sure to configure your system so that the MIB Poller with MeterWare is the only one used.

The following steps describe how to ensure that the MeterWare MIB Poller is used when you have the Meter Reporting System installed on the same machine:

1. Copy the file **c:\natmrs\mibpoll\natmrs.mpf** to **c:\mtrware\mibpoll\natmrs.mpf**.
2. Confirm that the MibPoll dBase, dBase Driver, data source points to **c:\natmrs\mibpoll\data**.
3. Confirm that the MeterWare Device Data Source is pointing to **c:\mtrware\database**.

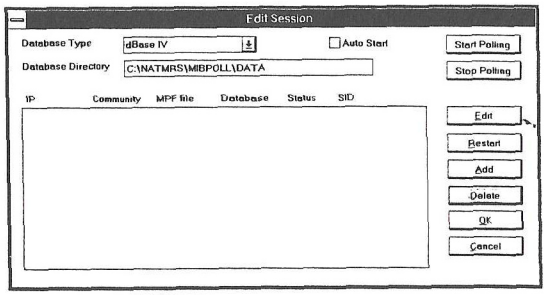
This allows only the Mib Poller from MeterWare to be used.

To collect data, do the following:

1. From the main menu, choose Tools/MIBPoller.

   Assuming you have no sessions of data defined, you arrive at the Edit Session window. (See Figure 6-7)

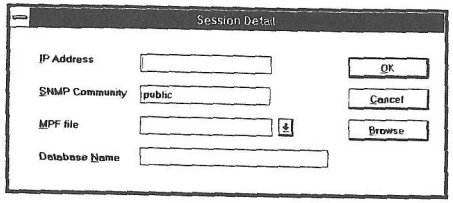
Figure 6-7 MIB Poller's Edit Session Window



2. Click on Add.

   The Session Detail window appears. (See Figure 6-8)

Figure 6-8 **Session Detail Window**



3. Type in (or select where applicable) the following information:
   - `IP Address`: The IP address of the meter.
   - ***`SNMP Community`***: Accept the default or type in one of your own.
   - **MPF File**: Click on the down arrow and select either *emeter.mpf* or *trmeter.mpf*.
   - *** For advanced users: After you add your session(s), you can use MIB Poller's Edit MPF option to create and define the contents of your **.mpf* files.
   - `Database Name`: Depending on which database you are using, this is either the name of the directory where your database tables (e.g., **.dbf*, **.txt*) are stored or the actual name of the file (e.g., *SAMPLE.mdb*).

The MPF file contains collections of MIB variables defined to be a group. The tables provided in either emeter.mpf or trmeter.mpf represent collections of MIB variables from the RMON Statistics, RMON Host and N. A. T. EtherMeter and TokenMeter groups.

4. Click on OK.

   You are returned to the Edit Session window. The session you just added appears in the window.

5. Click on the session's row and click on Start Polling.

   Assuming you have defined a valid data set, you will see Active in the Status column.

6. Click on OK.

   You are returned to the main MIB Poller window. The session you just created appears in the window.

7. After waiting for one or two polling intervals, click on the session's row.

   A listing of the database tables appears in the lower part of the main MIB Poller window.

8. Double–click on the row of a database table to access the Table Browser. (Please see the "Table Browser" help topic for more information.)

Enterprise View Window

The enterprise view screen shows the complete group of EtherMeter or TokenMeter probes in use on the enterprise network. Select up to 4 meters and then click the view button to see summary statistics on each segment or ring.

Docking Bar

The docking bar is located at the bottom of the main MeterWare window and provides place holders for active applets. A set of VCR style controls allows the user to move the selection of open applets.

Double-click an icon to make the window appear. Any open applet may be minimized to place its icon on the docking bar.

Dial Remote

Use the Tools/Dial Remote option for accessing devices over the PC's serial communications port. Modem and serial options for each device are configured in the Information and Configuration tab for each device.

Modem Trace

Use the Tool/Modem trace option for debugging problems with devices that you are accessing out-of-hand.

Non-portable character codes will not be displayed.

Chapter 7 BootP Name Server

The BOOTP Name Server assigns a device IP address, managing host IP address and default router IP address to managed N.A.T. devices. The MeterWare BOOTP Name Server can function in two ways:

- When assembling a network, you can create a list of Ethernet or Token Ring addresses to which you have assigned IP addresses.

  As you add a device and power it up, if there is no configuration data in the non-volatile memory area, the device broadcasts BOOTP requests at regular intervals. If the BOOTP Name Server is active and sees a BOOTP request from a device in its table, it responds to the request, downloading the preset configuration data.

- The configuration data can be forced into a device using a SET command.

  If the device contains configuration data and you want to overwrite the IP address, managing host and default router IP address (where applicable) you can enter the data and download it to the device.

Once the IP address, managing host and router IP address are established, MeterWare's Edit Device feature can be used to change the other configuration parameters. (All other parameters are reset to the manufacturer's defaults.)

WARNING: ***If the device has already been configured through its serial port and has parameter information stored in its non-volatile memory, be careful. This command erases all configuration information in the device's non-volatile memory.***

Router Considerations

A BOOTP request is a broadcast packet originated by a device and cannot be forwarded by a router unless the router can be configured with a "helper" address. If a router does not have helper address functionality, it does not forward the BOOTP request packet nor do the SET operations used by the BOOTP Name Server work.

When such "helper" capability is configured, the BOOTP requests generated by N.A.T. devices are routed to the server, and the replies routed back to the devices.

If the device and the managing host are on the same LAN segment (no router between the managing host and the managed device), no special consideration is required. Where two LANs are joined by a bridge that is transparent to the system, again no special consideration is required.

In other words, there must be a direct path between the managing host and the managed device. That path may include MAC-layer bridges, but not IP routers. If there is a router between the managing host and the managed device, the router's IP address must be specified. If the router does not have "helper address" functionality, the device can be temporarily relocated to a local connection, configured with an ASCII terminal or accept data from another BOOTP server.

Although physically relocating the device may be inconvenient, it is easy to configure the device through MeterWare using a temporary IP address. With the configuration data stored in the device's non volatile memory area, the device can then be relocated to its permanent location. When the device is powered up, it reads the configuration data from the non volatile memory area and responds accordingly.

ASCII terminal configuration is discussed in the user's guide supplied with the device.

BOOTP Device Configuration

You can build a table to answer BOOTP requests. This is especially useful if you are adding several devices to the network. It automates the process of assigning IP addresses to devices.

You can create a list of IP addresses assigned to Ethernet addresses, then add a device to the network. If there is no configuration data in the non-volatile memory area, the device broadcasts BOOTP requests. If the BOOTP Name Server sees a BOOTP request, it responds to the request, downloading the preset configuration data from MeterWare to the device.

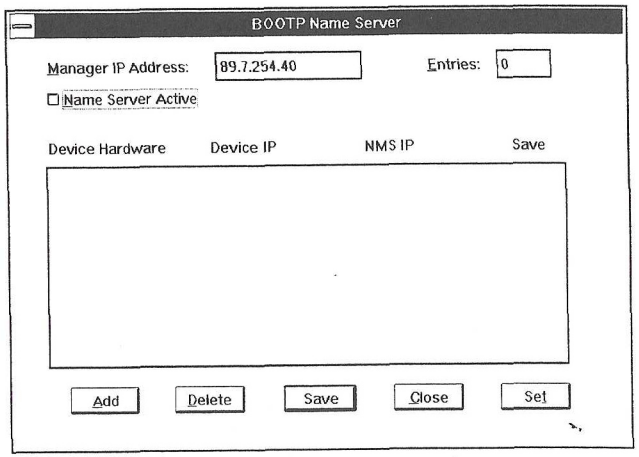
The configuration data can also be forced into a device using a SET command. This is useful when you want to change the IP address of a device that already has configuration data or you do not want to wait for the BOOTP request.

Add Devices to the BOOTP Table

To add device parameters to the BOOTP Name Server table, complete the following procedure.

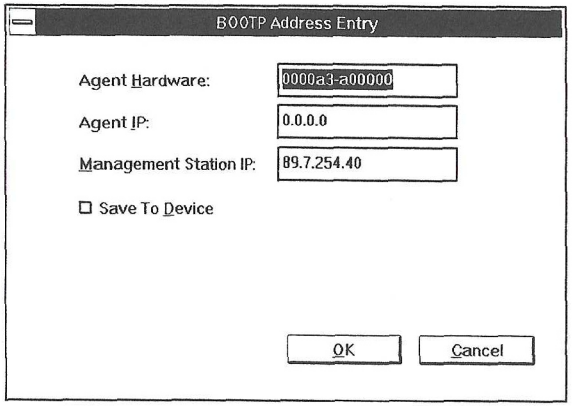
1. Choose BOOTP Editor from the Options menu.
   The BOOTP Name Server window. See Figure 7-9.

Figure 7-9 BOOTP Name Server Window



2. Make sure the name server is active. If necessary, click in the Name Server Active box until an X appears. If the BOOTP Name Server is not active, it does not respond to BOOTP requests. The Name Server Active box does not have to be checked to force an IP address download.
3. Click Add to display the BOOTP Address Entry window. See Figure 7-10.

Figure 7-10 BOOTP Address Entry Window



4. Type the <Ethernet or Token Ring MAC address> of the device in the Agent hardware field. The Agent Hardware address is the device's Ethernet address. If you selected a device before opening the window, the system enters the Ethernet address for the selected device.
5. Type the <IP address> for the device in the Agent IP field.
6. Type the <IP address> of the managing station in the Management Station IP field. The field defaults to the IP address of your MeterWare station.

   At this point, the data is scheduled to be downloaded into the device's RAM memory area upon detecting a BOOTP request for the Ethernet address (agent hardware) specified. When the BOOTP Name Server responds to a BOOTP request, the data is not saved into the device's non-volatile memory area. If the device is reset (powered off and on), the device reverts to its status before the BOOTP Name Server downloaded the data.

7. Continue with the next section to save the data to the device's non-volatile memory area.

   — OR —

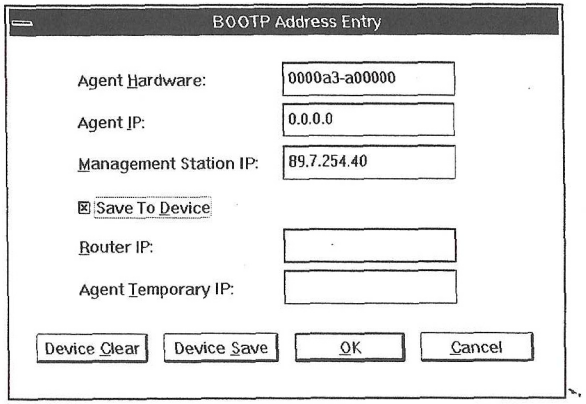
   Click OK to return to the BOOTP Name Server window.

Save Configuration Data to Non-volatile Memory

To save the configuration data permanently to the non volatile memory area of the device, complete the following procedure:

1. Click the box in front of the Save in device option field to display the additional BOOTP parameters. See Figure 7-11.

Figure 7-11 Extended BOOTP Address Entry Window



2. Type the [IP address] of the router in the Router IP field.

   If the device is on the same LAN segment, this field may be left blank. If the device is on another LAN segment, connected by a router capable of forwarding BOOTP request packets, enter the IP address of the router.

3. Type a [temporary IP] address for the device in the Agent Temporary IP field.

   The temporary IP address is loaded into the RAM memory area of the device. It is not loaded into the non volatile memory area. The data in the Agent IP field is loaded into non volatile memory. Therefore, if you are configuring the device on a local LAN with the intent of moving the device to another LAN, use the temporary IP address to identify the device. When the device is power cycled, the IP address stored in the non volatile memory area is loaded into the RAM area.

4. Click Device Save.
5. Click Done to exit.

   Within approximately two minutes after the name server entries are complete and the devices are powered on, the configuration data is sent to the devices.

   If a device is preconfigured, attached to an active network and powered up, it DOES NOT issue a BOOTP request. The only devices that issue BOOTP requests are those without an IP address. If you want to gain control of a device through MeterWare, you can force a configuration download, as described in the next section.

NOTE: If the icon does not appear, it is likely the MAC address was entered incorrectly or the router is not forwarding the response. On N.A.T. devices the MAC address is located on the bottom of stand alone devices and on the backing plate of MUE rack mount devices.

Force Configuration Data Download

Configured devices do not broadcast BOOTP requests. To assign an IP address and gain control of a device, it is necessary to force a download of the configuration data. This feature is useful if the device was configured on another network or for other tasks at a remote site.

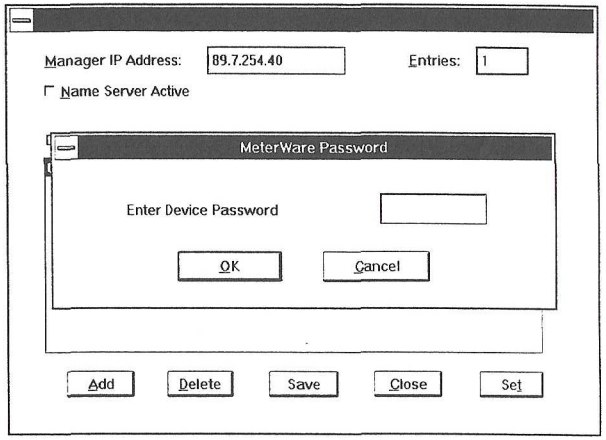
N.A.T. devices have a password protection feature that limits the ability of the BOOTP Name Server to issue a SET command. The device password prevents an unauthorized person from "taking over" a device.

To force the downloading of configuration data, complete the following procedure:

1. Complete the procedures described in the previous two sections to add the device to the BOOTP Name Server table.
2. Click the table entry for the device.
3. Click Set.

   You are prompted for the password. See Figure 7-12.

Figure 7-12 Password Window Under BOOTP Name Server



4. Type the <device password> if a password is assigned to the device.
   — OR —

   If a password has not been assigned, simply press RETURN.

   MeterWare sends the data to the device. MeterWare notifies the user that the configuration data has been sent, and that it takes about two minutes to record the change.

NUMERIC	NAME	NUMERIC	NAME
00-20-d4	ZEITNET	00-c0-75	XANTE
00-20-d5	VIPA	00-c0-76	IDATA
00-20-d6	LANNAIR	00-c0-77	DAEWOO
00-20-d7	JAPANMin	00-c0-78	COMPENGR
00-20-d9	PANASON	00-c0-79	FONSYS
00-20-da	XYLAN	00-c0-7a	PRIVA
00-20-db	XNET	00-c0-7d	RISC
00-20-dc	DENSITR	00-c0-7f	NUPON
00-20-dd	AWA	00-c0-80	NETSTAR
00-20-de	JAPANDIG	00-c0-81	METRODAT
00-20-df	KYOSAN	00-c0-82	MOORE
00-20-e0	PREMAX	00-c0-84	DATALINK
00-20-e1	ALAMAR	00-c0-86	LYNK
00-20-e2	INFORES	00-c0-87	UUNET
00-20-e3	KENCOM	00-c0-89	TELINDUS
00-20-e6	LIDKOPI	00-c0-8a	LAUTERBA
00-20-e7	B&W	00-c0-8b	RISQ
00-20-e8	DATATREK	00-c0-8c	PERF
00-20-e9	DANTEL	00-c0-8d	TRONIX
00-20-ea	EFFICIE	00-c0-8e	NIT
00-20-eb	CINCINN	00-c0-8f	MATSUSH
00-20-ec	TECHWARE	00-c0-90	PRAIM
00-20-ed	GIGABYTE	00-c0-91	JABIL
00-20-ee	GTECH	00-c0-92	MENNEN
00-20-ef	USC	00-c0-93	ALTA
00-20-f1	ALTOS	00-c0-96	TAMURA
00-20-f2	MAXIMUM	00-c0-97	ARCHIPEL
00-20-f3	RAYNET	00-c0-98	CHUNTEX
00-20-f4	SPECTRIX	00-c0-99	YOSHIKI
00-20-f5	PANDACOM	00-c0-9b	RELIANCE
00-20-f6	NETTEK	00-c0-9c	TOA
00-20-f7	CYBERDAT	00-c0-9d	DISTR
00-20-f8	CARRERAS	00-c0-9f	QUANTA
00-20-f9	PARALINK	00-c0-a0	ADVMICRO

NUMERIC	NAME	NUMERIC	NAME
00-20-fa	GDE	00-c0-a1	TOKYO
00-20-fb	OCTEL	00-c0-a2	INTERMED
00-20-fc	MATROX	00-c0-a3	DUAL
00-20-fd	ITV	00-c0-a4	UNIGRAF
00-20-fe	TOPWARE	00-c0-a7	SEEL
00-20-ff	SYMMET	00-c0-a8	GVC
00-40-01	ZEROONE	00-c0-a9	BARRON
00-40-09	TACHIBAN	00-c0-aa	SILVAL
00-40-0c	GENMICRO	00-c0-ab	JUPITER
00-40-0d	LANNET	00-c0-ac	GAMBIT
00-40-10	SONIC	00-c0-ad	MARBEN
00-40-13	NTT	00-c0-ae	TOWERCOM
00-40-14	COMSOFT	00-c0-af	TEKLOGIX
00-40-15	ASCOM	00-c0-b0	GCCINC
00-40-1f	COLGRAPH	00-c0-b2	NORAND
00-40-20	PINACL	00-c0-b3	COMSTAT
00-40-23	LOGIC	00-c0-b4	MYSON
00-40-25	MOLDyn	00-c0-b5	CORPNET
00-40-26	MELCO	00-c0-b6	MERIDIAN
00-40-27	SMC	00-c0-b7	AMPWRCON
00-40-2a	CANOGA	00-c0-b8	FRASER
00-40-2f	XLNT	00-c0-b9	FUNK
00-40-30	GK	00-c0-ba	NETVANTA
00-40-32	DIGITAL	00-c0-bb	FORVAL
00-40-33	ADDTRON	00-c0-bd	INEX
00-40-39	OPTEC	00-c0-be	ALCATEL
00-40-3c	FORKS	00-c0-bf	TECHCONC
00-40-3f	SSANGYON	00-c0-c0	SHORE
00-40-41	FUJIKURA	00-c0-c1	QUADGRAH
00-40-43	NOKIA	00-c0-c2	INFINITE
00-40-48	SMD	00-c0-c3	ACUSON
00-40-4c	HYPERTEC	00-c0-c4	COMPOPER
00-40-4d	TELETECH	00-c0-c5	SID
00-40-4f	NAVALWAR	00-c0-c6	PERSMEDI

NUMERIC	NAME	NUMERIC	NAME
00-40-50	IRONIC	00-c0-c8	MICROBYT
00-40-52	STAR	00-c0-c9	BAILEY
00-40-54	THINKMAC	00-c0-ca	ALFA
00-40-57	LOCKHEED	00-c0-cb	CNTRLRAT
00-40-59	YOSHIDA	00-c0-cd	COMELTA
00-40-5b	FUNASSET	00-c0-d0	RATOC
00-40-5d	STARTEK	00-c0-d1	COMTREE
00-40-66	HITACHI	00-c0-d2	SYNTELL
00-40-67	OMNIBYTE	00-c0-d4	AXON
00-40-68	EXTENDED	00-c0-d5	QUANCOM
00-40-69	LEMCOM	00-c0-d6	J1
00-40-6a	KENTEK	00-c0-d9	QUINTE
00-40-6e	COROLLAR	00-c0-db	IPC
00-40-6f	SYNC	00-c0-dc	EOS
00-40-74	CABLEWIR	00-c0-de	ZCOMM
00-40-76	AMPR	00-c0-df	KYE
00-40-78	WEARNES	00-c0-e1	SONIC
00-40-7f	AGEMA	00-c0-e2	CALCOMP
00-40-82	LAB	00-c0-e3	OSITECH
00-40-85	SAAB	00-c0-e4	LANDIS
00-40-86	MICHELS	00-c0-e5	GESPAC
00-40-87	UBITREX	00-c0-e6	TXPORT
00-40-8a	TPS	00-c0-e7	FIBERDAT
00-40-8c	AXIS	00-c0-e8	PLEXCOM
00-40-8e	Digilog	00-c0-e9	OAK
00-40-8f	WMDATA	00-c0-ea	ARRAY
00-40-91	PROCOMP	00-c0-eb	SEHTECHN
00-40-92	ASP	00-c0-ec	DAUPHIN
00-40-94	SHOGRAPH	00-c0-ed	USARMY
00-40-95	RPT	00-c0-ee	KYOCERA
00-40-96	TELESYS	00-c0-ef	ABIT
00-40-98	DRESSLER	00-c0-f0	KINGSTON
00-40-9a	NETExp	00-c0-f1	SHINKO
00-40-9c	TRANSWAR	00-c0-f2	TRANSENG

NUMERIC	NAME	NUMERIC	NAME
00-40-9d	DIGIBOAR	00-c0-f3	NETWORK
00-40-9e	CONCURRE	00-c0-f4	INTERLNK
00-40-9f	LANCAST	00-c0-f5	METACOMP
00-40-a4	ROSE	00-c0-f6	CELAN
00-40-a6	CRAYRES	00-c0-f7	ENGAGE
00-40-aa	VALMET	00-c0-f8	ABOUT
00-40-ad	SMA	00-c0-f9	HARRIS
00-40-ae	DELTA	00-c0-fa	CANARY
00-40-b4	3COMKK	00-c0-fb	ADTECHL
00-40-b5	VIDEOS	00-c0-fc	ELASTIC
00-40-b6	COMPUTERM	00-c0-fd	PROSUM
00-40-b9	MACQ	00-c0-ff	BOXHILL
00-40-bd	STARLIGH	01-00-5e	DODINET
00-40-c0	VISTA	02-07-01	RACAL
00-40-c1	BIZERBA	08-00-07	APPLE
00-40-c2	ACD	08-00-09	HP
00-40-c3	FISCHER	08-00-0b	UNISYS
00-40-c6	FIBERNET	08-00-0d	ICL
00-40-c8	MILAN	08-00-17	NATSEMI
00-40-cc	SILCOM	08-00-1f	SHARP
00-40-cf	STRAWTRE	08-00-20	SUN
00-40-d2	PAGINE	08-00-28	TEXAS
00-40-d4	GAGE	08-00-2b	DEC
00-40-d7	STUDIOGE	08-00-30	CERN
00-40-d8	OCEANOFF	08-00-32	TIGAN
00-40-dc	TRITEC	08-00-39	SPIDER
00-40-df	DIGALOG	08-00-48	EUROTHER
00-40-e1	MARNER	08-00-51	EXPERDAT
00-40-e2	MESARIDG	08-00-5a	IBM
00-40-e3	QUIN	08-00-69	SGI
00-40-e4	EM	08-00-74	CASIO
00-40-e5	SYBUS	08-00-8f	CHIPCOM
00-40-e7	ARNOS	10-00-5a	IBM
00-40-e9	ACCORD	aa-00-00	DEC

NUMERIC	NAME	NUMERIC	NAME
00-40-ea	PLAINTRE	aa-00-03	DEC
00-40-ed	NETCTLS	aa-00-04	DEC

Appendix B NAC/102 Installation

MeterWare can use N.A.T.'s NAC/102 Ethernet adapter card to communicate with the network. The NAC/102 card can be installed in any open 16 bit bus slot. This chapter describes how to install N.A.T.'s Ethernet adapter card.

The MeterWare installation program runs a diagnostic program on the N.A.T. Ethernet adapter card. If an error message is displayed, go back and correct the Ethernet adapter problem before proceeding.

NOTE: Users with Ethernet Adapter card NAC/101 or NAC/100 must upgrade their Ethernet Adapter card to an NAC/102. Contact N.A.T. Customer Service for details at (408) 370-4300 or service@nat.com.

All switches and jumpers not mentioned in this text are set by the factory and should not be changed.

NAC/102 Jumper Settings

The hardware configuration of the NAC/102 is set at the factory for most MeterWare applications. Jumper block identification is stenciled on the PC board beside the block's location. N.A.T.'s default configuration is shown in the table below.

BLOCK	SETTING	DESCRIPTION
E2	Pins 1 & 2 closed.	Thin Ethernet interface active
E3	E3-6 & E3-8 closed.	I/O address 0x0340h through 0x035Fh
E4	IRQ5	Interrupt 5

The Ethernet adapter's I/O address is defined by jumper block E3, positions 4 through 8. The adapter requires a 32 byte block at the selected address. If there is a suspected conflict with the I/O address, the table below shows alternative settings.

I/O ADDRESS	E3-4	E3-5	E3-6	E3-7	E3-8
0x0000h	Closed	Closed	Closed	Closed	Closed
0x0020h	Closed	Closed	Closed	Closed	Open
0x0040h	Closed	Closed	Closed	Open	Closed
0x0060h	Closed	Closed	Closed	Open	Open
0x0080h	Closed	Closed	Open	Closed	Closed
0x00A0h	Closed	Closed	Open	Closed	Open
0x00C0h	Closed	Closed	Open	Open	Closed
0x00E0h	Closed	Closed	Open	Open	Open
0x0100h	Closed	Open	Closed	Closed	Closed
0x0120h	Closed	Open	Closed	Closed	Open
0x0140h	Closed	Open	Closed	Open	Closed
0x0160h	Closed	Open	Closed	Open	Open
0x0180h	Closed	Open	Open	Closed	Closed
0x01A0h	Closed	Open	Open	Closed	Open
0x01C0h	Closed	Open	Open	Open	Closed
0x01E0h	Closed	Open	Open	Open	Open
0x0200h	Open	Closed	Closed	Closed	Closed
0x0220h	Open	Closed	Closed	Closed	Open
0x0240h	Open	Closed	Closed	Open	Closed
0x0260h	Open	Closed	Closed	Open	Open

I/O ADDRESS	E3-4	E3-5	E3-6	E3-7	E3-8
0x0280h	Open	Closed	Open	Closed	Closed
0x02A0h	Open	Closed	Open	Closed	Open
0x02C0h	Open	Closed	Open	Open	Closed
0x02E0h	Open	Closed	Open	Open	Open
0x0300h	Open	Open	Closed	Closed	Closed
0x0320h	Open	Open	Closed	Closed	Open
0x0340h*	Open	Open	Closed	Open	Closed
0x0360h	Open	Open	Closed	Open	Open
0x0380h	Open	Open	Open	Closed	Closed
0x03A0h	Open	Open	Open	Closed	Open
0x03C0h	Open	Open	Open	Open	Closed
0x03E0h	Open	Open	Open	Open	Open

*default

NOTE: If you are not using the default, add "Set NACIOP=OXaddr." to your autoexec.bat file.

Ethernet Interface

The NAC/102 supports a Thin Ethernet interface with a BNC connector or a Thick Ethernet AUI interface.

Jumper block E2 selects the active Ethernet interface. N.A.T.'s standard configuration is Thin Ethernet through the BNC connector. If a Thick Ethernet interface is used through the 15-pin AUI connector, the jumper must be repositioned.

INTERFACE	CONNECTOR	JUMPER BLOCK E2
Thin Ethernet	BNC	Pins 1 and 2 are closed.
Thick Ethernet	AUI	Pins 2 and 3 are closed.

Interrupt Request (IRQ) Settings

I/O ports communicate through interrupts. The number of interrupts is limited and subject to conflicts.

The standard configuration for PC serial ports is IRQ4 for COM1 and COM3, and IRQ3 for COM2 and COM4. IRQ4 and IRQ3 can be used for the NAC/102 card, but the conflicting I/O ports must be disabled. Commonly, jumpers on an I/O card plugged into the PC bus control the COM and LPT port configuration for that card.

LPT2 (Printer Port 2) is commonly set to IRQ5. The standard setting for the N.A.T. Ethernet adapter card is IRQ5. If LPT2 is installed, it will conflict with this setting. Disable the LPT2 port or change the interrupt setting for the Ethernet adapter.

If a bus mouse is used, it will have a small adapter board that requires a dedicated IRQ. Follow the vendor's installation instructions to assign a unique IRQ to the mouse board. In some cases, you may have to disable COM1 or COM2 and assign the bus mouse to IRQ4 or IRQ3.

Verify that no other boards might create interrupt conflicts. A commonly overlooked board is a modem. Consult the manufacturer's instructions regarding IRQ settings.

Appendix C Your MTRWARE.INI File

When you first start MeterWare, you must select the IP stack you are using. After making a selection, your *mtrware.ini* file (located in the *mtrware\bin* directory) is updated to reflect the IP stack you are using.

The following information appears in a typical *mtrware.ini* file.

```
[ACTIVE TCPIP]
;ACTIVE=WSK2NIL.DLL - for generic winsock
ACTIVE=FTP2NIL.DLL - for ftp software
;ACTIVE=NMG2NIL.DLL - for Netmanage

[VENDER TCPIP]
NAT (Ethernet Only)=NAT2NIL.DLL
FTP=FTP2NIL.DLL
NetManage=NMG2NIL.DLL
WinSock Only=WSK2NIL.DLL
```

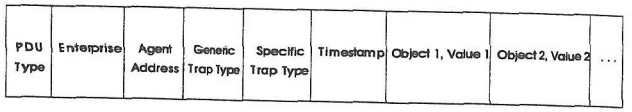
NOTE: BOOTP will only work with N.A.T. NAC/102 and NetManage stack. Ping works with N.A.T., NetManage and FTP. For example, if you are using NetManage, the [ACTIVE TCPIP] section of your *mtrware.ini* file would look like the following:

```
[ACTIVE TCPIP]
ACTIVE=NMG2NIL.DLL
```

Appendix D Traps

The Trap PDU has a format distinct from the four other SNMP PDUs. The first field indicates the Trap PDU and contains PDU Type = 4. The Enterprise field identifies the management enterprise under whose registration authority the trap was defined. The Agent Address field, which contains the IP address of the agent, provides further identification. See Figure D-1.

Figure D-1 SNMP Trap PDU Structure



The Generic Trap type provides more specific information on the event being reported. There are seven defined values (enumerated INTEGER types) for this field:

GENERIC TRAP	VALUE	MEANING
coldStart	0	The sending protocol entities (higher layer network management) has reinitialized, indicating that the agent's configuration nor entity implementation can be altered.
warmStart	1	The sending protocol has reinitialized, but neither the agent's configuration or the protocol entity implementation has altered.
linkDown	2	A communication link has failed. The affected interface is identified as the first element within the variable bindings field: name and value of the ifIndex instance.
linkUp	3	A communication link has failed. The affected interface is identified as the first element within the variable bindings field: name and value of the ifIndex instance.

GENERIC TRAP	VALUE	MEANING
authentificationFailure	4	The agent has received an improperly authenticated SNMP message from the manager; that is, the community name was incorrect.
egpNeighborLoss	5	An EGP peer neighbor is down.
enterpriseSpecific	6	A nongeneric trap has occurred, which is further identified by the Specific Trap Type field and Enterprise field.

The two additional fields complete the Trap PDU. The Timestamp field contains the value of the sysUpTime object, representing the amount of time elapsed between the last (re-) initialization of the agent, and the generation of that Trap. The last field contains the Variable Bindings.

Enterprise Specific Traps

When the generic trap type is = 6 (enterpriseSpecific) then the combination of Enterprise and the specific trap type indicate which trap is being sent.

Traps Defined for the RMON Group

Enterprise: 1.3.6.1.2.1.16 - rmon

Content: variables in the RMON alarm or filter group

SPECIFIC TRAP CODE	TYPE	GENERATOR
1	rising alarm	RMON alarm
2	falling alarm	RMON alarm
3	channel match	RMON filter

Traps Defined for N.A.T.

Enterprise: 1.3.6.1.4.1.86.1.2 - products.2

SPECIFIC TRAP CODE	TYPE	GENERATOR
22	Bad Authentication	SNMP
49	frame count alert	N.A.T. alert
50	broadcast count alert	N.A.T. alert
51	multicast count alert	N.A.T. alert
52	error count alert	N.A.T. alert
53	utilization count alert	N.A.T. alert
54	duplication ip address	N.A.T. mapping
55	ip address change	N.A.T. mapping
56	top10 nodes exceed the threshold	N.A.T. top10
58	new node detection	N.A.T. NND
59	heartbeat	N.A.T. sap check
60	shoulder tap	N.A.T. shoulder tap - ping test
61	snmp polling	N.A.T. S.P.E.

Glossary

10Base-T An Ethernet Unshielded Twisted Pair (UTP) interface. The 10Base-T standard limits UTP (i.e., telephone wire) segments to 100 meters (328 feet) in length.

Access Level The permission level granted by an SNMP community.

Address Resolution Protocol (ARP) The protocol used to map IP addresses to physical Ethernet addresses.

Advertising The process whereby routers periodically send out their latest routing information.

Agent In the context of N.A.T.'s User's Guides, agent is referred to in the context of an SNMP agent. An SNMP agent is software that resides in a device (or managed system) on the network.

Asymmetrical In the context of N.A.T.'s User's Guides, it means that the bridge can transmit data at one speed and receive data at a different speed.

Attachment Unit Interfaces (AUI) Attachment Unit Interface. Standard IEEE 802.3 or Ethernet interface, often called "thick Ethernet." This interface uses a 15-pin "D" connector which is attached to an external transceiver through a shielded cable up to 50 meters (164 feet) in length.

Bindery A database of resources and clients on a network.

BOOTP Name Server A network server for IP protocols which, among other functions, assigns host IP addresses based on physical Ethernet addresses.

Bridging Network Control Protocol (BNCP) A network layer protocol used for establishing non-IP communication (bridging) over serial link connections.

Cheapernet A popular term for Thin Ethernet.

Click To press and release the mouse button.

Client Client refers to the "client" in the "client/agent model." The client (more commonly referred to as the manager) is the network management station that sends control commands to the agent.

Community String Community strings serve as "passwords" for SNMP messages. When an SNMP message is sent to a device, the device verifies whether or not the community string in its configuration matches that of the SNMP message being sent. If the community string is correct, the device will respond.

Configuration Cable A cable that links a network device for the purposes of configuration or communications. Configuration cables come in several forms.

Custom Filtering A function provided by N.A.T. management bridges which controls the types of packets which are forwarded by the bridge. This feature may be used to control forwarding by packet type, protocol type, station address or other user-specified criteria. It is most often used to establish access security, creating "closed user groups" in the LAN inter-network which cannot be reached by unauthorized users.

Cyclic Redundancy Check (CRC) A cyclic redundancy check error polynomial appended to each Ethernet packet to verify that no errors were introduced during transmission.

Delta Rate The average result for a given statistic, over a given sampling interval, as opposed to taking a sampling at a narrow peak.

Data Circuit Terminating Equipment (DCE) The devices in a network that connect the communication circuit with the end device or DTE (data terminal equipment). A modem is a DCE to an analog network; a CSU/DSU is a DCE to a digital network.

Data Packet A group of bits that make up one network transmission.

Dataphone Digital Service (DDS) An AT&T Communications service which eliminates the need for modems, since data is transmitted in digital rather than analog form.

DSAP Destination Service Access Point.

Data Terminal Equipment (DTE) User devices, such as an EtherMeter, that connect to data communications equipment. DTE's receive and generate data carried by the network.

Delimiter A single character used in a command string that marks the beginning or end of a unit of data.

Drop-down Menu A subordinate menu or list of options that appears below its parent menu.

Enterprise Number N.A.T.'s enterprise number is 86. It is a unique number assigned to an institution for use in defining proprietary extensions to the standard Internet MIB.

FLASH FLASH refers to a type of non-volatile Random Access Memory (NV_RAM). It is electrically erasable so new data can replace (overwrite) old data. FLASH memory eliminates the need to dismantle the unit and replace PROM chips for the purpose of updating firmware code. New code is easily downloaded into the FLASH memory area of the device.

Fly-out Menu A subordinate menu or list of options that appears to the side of its parent menu.

Gateway A gateway is a communications device which is used to connect dissimilar types of network protocols. Gateways translate information and forward data between network protocols.

High-Level Data Link Control (HDLC) HDLC is a bit-oriented line protocol specification published by the Internet Standards Organization (ISO) as ISO 3309 and ISO 4335.

Icon A picture or drawing that represents an application program or device.

Icon Management The POLYCENTER SNMP Manager's Icon Manager function is used to customize the icons displayed on the map screen to suit user-specific needs.

In band Communications Data transfer that occurs between devices connected to the same LAN. For example, if a PC sends a packet to another PC across remote bridges communicating through modems, the connection between the PC and the bridge is in band. The modem connection is out of band.

Internal Port The link between the chip that controls the ports and the CPU.

Internet Control Message Protocol (ICMP) A protocol in an IP network that is used to perform control functions and report error messages.

Internet Protocol Control Protocol (IPCP) A network layer protocol used for establishing communication over the serial link connection.

Internetwork Packet Exchange (IPX) IPX is a connectionless protocol. It does not require acknowledgment by an IPX partner before sending data and there is no guarantee of delivery.

Jabber Protect Condition Automatically interrupts the transmit function and inhibits an abnormally long output data stream.

Keywords Menu headings which are found in the title bar at the top of the window screen. Keywords are menu headings that when pointed to allow the user access to sub menu options.

Link Control Protocol (LCP) A link layer protocol used to establish, configure and test the data-link connection.

Main Window The single window that is the starting point for all interaction with an application.

Management Information Base (MIB) A collection of objects that can be accessed via a network management protocol.

Menu	A list from which you can choose one or more items.
Menu Bar	A horizontal area on a window that contains the names of pull-down menus.
NetWare Core Protocol (NCP)	NCP is the language that NetWare clients and servers "speak." Workstations transmit NCP messages to request file reads and writes, create queue jobs, determine drive mappings set and search large directories.
Network/Subnet Mask	A 32-bit quantity, in decimal dot notation, e.g., 255.0.0.0, indicating which bits in an IP address refer to the network portion.
Owner	The administratively assigned name of the owner that configured this entry and is therefore using the resources assigned to it. For example, RMON History can be monitored by several individuals at the same time, using different configuration parameters. Each individual can quickly identify which samplings are theirs by referring to the "Owner" field.
Out of band Communications	Data transfer that occurs outside of the LAN. For example, if two bridges transfer data through modems, the modem connection is considered to be out of band.
Point-to-Point Protocol (PPP)	The LANB/290 uses the PPP protocol to establish communication on its serial link.
Pop-Up Menu	A menu that appears on the screen when you select a particular function. It is a context-sensitive menu.
Request For Comments (RFC)	A document series that defines the Internet suite of protocols and related experiments.
Routing Information Protocol (RIP)	Routing information is contained in routing tables stored in each router and server. The routing information is passed between servers and routers using RIP. The protocol used by IP routers to exchange routing information with other routers on the network.
Remote Network Monitoring Management Information Base (RMON MIB)	The RMON MIB is a new SNMP standard for network monitoring. It is defined by RFC 1757 and RPC 1513.
Sampling Interval	The period of time over which the data is sampled. Usually used with EtherMeters to take a sampling at a given point in time.
Service Advertising Protocol (SAP)	SAP provides information regarding all the known servers on the entire network. The server name and type number are advertised throughout the network and stored in each server's bindery.

Static Route	A route that satisfies user-specified requirements. A static route consists of three components: IP address of the route, the IP address of the next hop and the metrics of the route.
Segment	A section of an Ethernet network consisting of an Ethernet cable up to 500 meters long.
Simple Network Management Protocol (SNMP)	A network management protocol that defines the communication between an addressable network object and its manager.
Sequenced Packet Exchange (SPX)	A connection oriented communications protocol that requires an SPX partner to be available before data is sent. SPX is slower than IPX communications because the sending device requires an acknowledgment, packets have a greater overhead (12 bytes) and are sent in sequence.
SSAP	Source service access point.
Spanning Tree Protocol	A protocol used by bridges which allows networks to be configured with redundant connections for increased reliability. Spanning Tree Protocol is used to prevent packets from being transmitted in loops through the redundant paths.
Sub menu	A menu that is displayed in response to dragging the mouse pointer over the cascade menu.
Subnet Mask	Subnet mask splits the IP address into two primary parts, the network identification (netid) and the host identification (hostid). The subnet mask specifically identifies how many of the 32 bits are dedicated to the netid and how many are dedicated to the hostid. The subnet mask on N.A.T. devices defaults to 255 netids and 16,777,215 hostids. The structure for the default subnet mask is 255.00.00.00. Basically, the high-order bits determine the number of netids and the remainder is dedicated to the hostids. For example, a subnet mask of 255.127.00.00 is acceptable. The bit pattern would be 11111111.01111111.00000000.00000000..
Thin Ethernet	Ethernet protocols may operate at standard speeds for reduced distances using thinner, less expensive and more easily installed coaxial cable. Thin Ethernet cable can be run up to 185 meters (606 feet).
Transmission Control Protocol/ Internet Protocol (TCP/IP)	Software for host-to-host communications and network packet formatting and addressing.
Traps	Traps are SNMP messages that are generated by an SNMP agent and automatically sent to a pre-defined host(s) on the network.

User Datagram Protocol/Internet Protocol (UDP/IP)	This protocol is used by SNMP agents and managers to communicate on a network.
Window	A rectangular ("box-like") region on the screen you use to interact with the application.

Index

Numerics

10Base-T
  definition, 169

802.3/SNAP
  IEEE, 71

A

access level
  definition, 169

accessing
  N.A.T.-specific applications, 62

accessing RMON MIB groups, 23

adding addresses to
  router tables, 67

adding devices
  to the BOOTP table, 133

adding firmware defaults, 122

adding new node detection control entries, 63

adding NND control table entries, 34

address resolution protocol (ARP)
  definition, 169

advertising
  definition, 169

agent
  definition, 169

alarms
  RMON, 23

application software
  downloading, 120

applications
  N.A.T.-specific, 62

ASCII files, 114
  layout, 111

ASCII terminals, 15

ASN.1, 101

assigning device addresses, 15

asymmetrical
  definition, 169

AUI
  definition, 169

authentificationFailure, 166

AUTOEXEC.BAT, 3

B

bindery
  definition, 169

BNC connector, 161

BOOTP, 15
  configured devices, 17
  device configuration, 132
  non volatile memory, 135
  requests, 132
  router considerations, 132
  table, 15

BOOTP name server, 15, 16, 131
  definition, 169

BOOTP name servers, 131

BOOTP table, 15
  adding devices, 133

bridging network control protocol (BNCP)
definition, 169

bus mouse, 162

C

capture
RMON, 23

cheapernet
definition, 169

click
definition, 169

client
definition, 169

coldStart, 165

collision errors, 30

color codes
device status, 20

commands
get, 74
get-next, 74
set, 15, 74

communities
SNMP, 128

community string, 169

configuration, 13
BOOTP, 15
device, 13
forced data download, 136
NAC/102 network cards, 13
system, 13
WINSOCK, 13–14

configuration cable
definition, 170

configuration data
devices, 17

configuring a non-SNMP device, 22

connecting devices, 21

control entries
new node detection, 63

control table variables
IP, 69

CRC align errors, 30

cyclic redundancy check (CRC)
definition, 170

D

data circuit terminating equipment (DCE)
definition, 170

data packet
definition, 170

data terminal equipment (DTE)
definition, 170

database names, 128

dataphone digital service (DDS)
definition, 170

dBase IV, 8

default router
IP address, 14

delimiter
definition, 170

delta rate
definition, 170

detecting duplicate addresses, 67

device configuration, 13
BOOTP, 132

device logs, 118
and searches, 118

device status, 20
blue, 20
green, 20
red, 20
yellow, 20

devices
configuration data, 17
connecting to network, 21
disconnecting, 21
locating, 22
removing, 21

dial remote, 129

directory
MTRWAREPL, 74

disk drives
floppy, 4

docking bar, 129

DOS 6.2, 3

downloading
application software, 120
firmware, 120

downloading firmware to devices, 122

draw palette, 19

drop event
errors, 31

drop-down menu
definition, 170

DSAP
definition, 170

duplicated IP addresses
detecting, 67

E

editing sessions, 127

egpNeighborLoss, 166

enterprise
windows view, 129

enterprise field identifies, 165

enterprise number
definition, 170

enterpriseSpecific, 166

error messages
firmware download, 124

error trend one view
statistics, 33

error trend two view
statistics, 34

error view
statistics, 30

Ethernet
RMON utilities, 25

Ethernet RMON utility
launching, 29

Ethernet types
name tables, 139

events
RMON, 23

F

files
ASCII, 114
ASCII layout, 111
firmware, 121
MTRWARE.INI, 121, 163
readme, 11

filter
RMON, 23

firmware
downloading, 120

firmware defaults
adding, 122

firmware download
error messages, 124

firmware files, 121

flash
definition, 170

fly-out menu
definition, 171

force configuration data download, 136

fragments
errors, 31

G

gateway, 13
definition, 171

generic Trap type, 165
graphical interface, 11
graphical network map, 11

H

hardware address, 14
help
  online, 13
helper address, 132
high-level data link control (HDLC)
  definition, 171
history
  RMON, 23
host
  RMON, 23
host window
  RMON, 34

I

ICMP echo packets
  see pings
icon
  definition, 171
icon management
  definition, 171
icons, 11
  and graphical network map, 11
  launching MeterWare, 11
  nodes, 11
  program group, 11
  readme, 11
  subnetworks, 11
identifying devices, 22
IEEE 802.3/SNAP, 71
in band communications
  definition, 171
information
  on Ethernet RMON utilities, 26
  on Token Ring utilities, 27
installation, 1
  BOOTP name server, 131
  ODBC overview, 3
  procedures, 3
installing MeterWare, 4–9
interfaces
  thin Ethernet
    NAC/102
      and thin Ethernet, 161
internal port
  definition, 171
internet control message protocol (ICMP)
  definition, 171
internet protocol control protocol (IPCP)
  definition, 171
internetwork packet exchange (IPX)
  definition, 171
interrupt request (IRQ) settings, 162
introduction, 1
IP (Internet Protocol)
  address, 14, 128
  assigning addresses, 15
  default router, 14
  gateway, 13
  mapping, 66
  pings, 20
  resolving addresses, 22
  router, 16
  specifying stacks, 12
  stack, 12
  subnet mask, 13, 14
IP mapping
  addresses, 66
  control entries, 66
  control table variables, 69
  MAC addresses, 66
IP mapping entries
  modifying, 68
IP stacks
  and MTRWARE.INI, 163
IRQ
  settings, 162

J

jabber protect condition
  definition, 171
jumper settings
  for NAC/102, 160

K

keywords
  definition, 171

L

LAN segments
  and BOOTP, 132, 135
Learn, 106
Learn Setup, 106
link control protocol (LCP)
  definition, 171
linkDown, 165
linkUp, 165
locating devices, 22, 116
  by IP address, 22
  by MAC address, 22
log dumps, 120

M

main window
  definition, 171
management information base (MIB)
  definition, 171
map, 18
mapping
  IP (Internet Protocol), 66
matrix
  RMON, 23
menu
  definition, 172
menu bar
  definition, 172
MeterWare
  graphical interface, 11
  icons, 11
  installing, 4–9
  package, 1
  setup, 4
  specifying IP stacks, 12
  system requirements, 3
MeterWare package, 1
MeterWare utilities
  listing of, 115
MIB compiler, 98–114
  limitations, 100
  name table, 114
  running, 100
MIB compiler messages, 100
MIB file format, 100
MIB poller, 127
MIB text format, 101
Microsoft's ODBC, 3
modem trace, 129
modifying
  IP mapping entries, 68
  new node detection control entries, 65
modifying log parameters, 118
MPF file, 128
MTRWARE.INI file, 163
MTRWAREPL directory, 74

N

N.A.T. extension
  RMON, 61
NAC/102
  jumper settings, 160

NAC/102 network cards, 13
name servers
  BOOTP, 16, 131
name table
  and numeric values, 139
name table dump, 112
name tables
  and ASCII files, 110
  customizing, 108
  editing, 110
  editing off-line, 110
  editing on-line, 109
  Ethernet types, 139
  sorting, 109
  vendor types, 146
netware core protocol (NCP)
  definition, 172
network cards
  NAC/102, 13
network manager, 12
network maps, 12, 18
  adding a sub-LAN, 20
  adding devices, 19
  connecting devices, 21
  locating devices, 22
  removing devices, 21
  tool palettes, 18
network palette, 18, 19
  connecting devices, 21
  disconnecting devices, 21
network/subnet mask
  definition, 172
networks
  connecting devices, 21
new node detection
  control table variables, 64
  table, 62
new node detection (NND)
  control table entries, 34
new node discovery, 62
NND
  see new node discovery
non volatile memory
  and BOOTP, 135
non-configured devices, 24
non-SNMP devices
  configuring, 22

O

ODBC
  configuration, 3
  dBase drivers, 7
  installing drivers, 3
  Microsoft, 3
  overview, 3
  setup, 3, 6
online help, 13
operations
  set, 91
out of band communications
  definition, 172
out-of-band
  communication, 13
oversize
  errors, 30
owner
  definition, 172

P

packet distribution
  statistics, 32
packet trend view
  statistics, 33
palettes, 18
  draw, 19
  network, 19
  tool, 18
parameters
  WINSOCK, 14
peak statistics, 69
pinging devices
  IP (Internet Protocol)

  ping, 126
pings, 20
point-to-point protocol (PPP)
  definition, 172
polling
  how to start, 128
pop-up menu
  definition, 172
program group, 11
protocol data unit (PDU)
  and traps, 165
protocols
  Ethernet, 71
  Token Ring, 71

R

RAM
  and BOOTP, 136
RARP
  server, 15
reactivating tables, 97
readme file, 11
remote network monitoring management information base (RMON MIB)
  definition, 172
removing devices, 21
request for comments (RFC)
  definition, 172
resolving IP addresses, 22
RMON
  accessing MIB groups, 23
  alarms, 23
  capture, 23
  events, 23
  filter, 23
  history, 23
  host, 23
  matrix, 23
  statistics, 23, 30
  Token Ring statistics, 23
  topN window, 35
RMON history window, 34
RMON host window, 34
RMON MIB
  N.A.T. extensions, 61
RMON MIB groups, 23
RMON Token Ring
  configuration, 23
  history, 23
  source routing, 23
  station, 23
  station order, 23
RMON utilities, 25
router considerations
  BOOTP, 132
router tables
  adding addresses to, 67
routing information protocol (RIP)
  definition, 172

S

sampling interval
  definition, 172
search options, 93
segment
  definition, 173
sequenced packet exchange (SPX)
  definition, 173
serial communications, 13, 14
serial ports
  and IRQ settings, 162
servers
  BOOTP, 15
service advertising protocol (SAP), 172
set command, 15